KVM over IP Switch
KN4164V / KN8132V / KN8164V

User Manual

www.aten.com

EMC Information

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

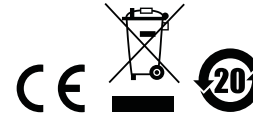
FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

CE Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

KCC Statement
유선 제품용 / A 급 기기 (업무용 방송 통신 기기)

이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .

Suggestion: Shielded twisted pair (STP) cables must be used with the unit to ensure compliance with FCC & CE standards.



RoHS

This product is RoHS compliant.

SJ/T 11364-2006

The following contains information that relates to China.

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
电器部件	●	○	○	○	○	○
机构部件	○	○	○	○	○	○

○: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006规定的限量要求之下。

●: 表示符合欧盟的豁免条款，但该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

×: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

User Information

Online Registration

Be sure to register your product at our online support center:

International	http://eservice.aten.com

Telephone Support

For telephone support, call this number:

International	886-2-8692-6959
China	86-10-5255-0110
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988
United Kingdom	44-8-4481-58923

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Battery Safety Notice

- There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the relevant instructions.

Batterie avis de sécurité

- Il existe un risque d'explosion si la batterie est remplacée par un incorrect tapez. Jeter les piles usagées selon la pertinente instructions.

Package Contents

The KVM over IP switch package consists of:

1 KN4164V / KN8132V / KN8164V Switch

2 Power Cords

1 Mounting Kit

2 Lok-U-Plugs

1 Lok-U-Plug Installation Tool

2 SA0142 Serial Adapters

1 Foot Pad Set (4 pcs.)

1 User Instructions*

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices on the installation.

***** Features may have been added since this manual was published. Please visit our website to download the most up to date version of the manual.

Copyright © 2015 ATEN® International Co., Ltd.

Manual Date: 2015-08-07

Altusen and the Altusen logo are registered trademarks of ATEN International Co., Ltd. All rights reserved.
All other brand names and trademarks are the registered property of their respective owners.

Contents

EMC Information ii
RoHS. iii
SJ/T 11364-2006. iii
User Information iv
Online Registration iv
Telephone Support iv
User Notice v
Battery Safety Notice. v
Batterie avis de sécurité v
Package Contents. vi
About This Manual xv
Overview xv
Conventions xvi
Terminology. xvii
Product Information. xvii

Chapter 1.
Introduction
Overview 1
Features 4
Hardware. 4
Management 4
Easy-to-Use Interface 5
Advanced Security 5
Virtual Media 6
Virtual Remote Desktop 6
KN8 V-Series Exclusive 6
System Requirements. 7
Remote User Computers. 7
Servers 7
KVM Adapter Cables. 8
Operating Systems 9
Browsers 9
Components 10
KN8132V Front View. 10
KN8164V / KN4164V Front View 10
KN8132V Rear View 13
KN8164V / KN4164V Rear View 13

Chapter 2.
Hardware Setup
Overview 15
Before You Begin 15
Stacking and Rack Mounting 16
Stacking. 16
KN8132V Rack Mounting 17
Rack Mounting - Front 17
Rack Mounting - Rear 19
KN8164V / KN4164V Rack Mounting 21

Rack Mounting - Front . . . 21
Rack Mounting - Rear . . . 23
Single Stage Installation . . . 25
Single Stage Installation Diagram . . . 27
Adapter Cable Connection Diagram . . . 28
Adapter Cable Connection Diagram cont. . . . 29
Two Stage Installation . . . 30
Two Stage Installation Diagram . . . 31
PDU Installation . . . 32
Hot Plugging . . . 34
The Adapter ID Function . . . 34
Powering Off and Restarting . . . 35
Port ID Numbering . . . 36
Port Selection . . . 36

Chapter 3.
Super Administrator Setup
Overview . . . 37
First Time Setup . . . 37
Network Setup . . . 39
Changing the Super Administrator Login . . . 40
Moving On . . . 42

Chapter 4.
Logging In
Overview . . . 43
Local Console Login . . . 43
Browser Login . . . 44
Windows Client AP Login . . . 45
The Windows Client AP Connection Screen . . . 46
Connecting – Windows Client AP . . . 47
The File Menu . . . 48
Java Client AP Login . . . 49
The Java Client AP Connection Screen . . . 50
Connecting – Java Client AP . . . 51

Chapter 5.
The User Interface
The Web Browser Main Page . . . 53
Page Components . . . 54
The Tab Bar . . . 55
The AP GUI Main Page . . . 56
The Local Console GUI Main Page . . . 58
The Control Panel . . . 59
WinClient Control Panel . . . 59
WinClient Control Panel Functions . . . 61
Macros . . . 64
Hotkeys . . . 64
User Macros . . . 66
System Macros . . . 70
Video Settings . . . 73

Gamma Adjustment 77
The Message Board 78
Button Bar 78
Message Display Panel 79
Compose Panel 79
User List Panel 79
Virtual Media 80
Mounting Virtual Media 80
Zoom 83
The On-Screen Keyboard 84
Changing Languages 84
Selecting Platforms 85
Expanded Keyboard 85
Mouse Pointer Type 86
Power Over the Net™ 87
Mouse DynaSync Mode 88
Automatic Mouse Synchronization (DynaSync) 88
Mac and Linux Considerations 89
Manual Mouse Synchronization 89
Control Panel Configuration 90
The Java Control Panel 92

Chapter 6. Port Access

Overview 93
Browser GUI 93
AP GUI 93
The Sidebar 95
The Sidebar Tree Structure 95
Scan 96
Array 96
Filter 97
Sidebar Utilities 98
Port/Outlet Naming 99
KVM Devices and Ports – Connections Page 101
Device Level 101
Port Level 102
Status 102
Associated Links 102
Power Management 103
PON Devices – Device Monitor Page 104
The Main Panel – PON View 104
Action Buttons 105
Outlet Groups 106
The Main Panel – Group View 107
Outlet Settings 108
Blade Servers – Connections Page 109
The Blade Configuration Page 109
Associating Ports 110
Main Panel Device View 110
Main Panel Blade View 111

Unassociating Ports . . . 112
History . . . 113
Favorites . . . 114
Adding a Favorite . . . 114
Modifying a Favorite . . . 116
User Preferences . . . 117
Sessions . . . 119
Access . . . 120
Device Level Browser GUI Interface . . . 120
Port Level Browser GUI Interface . . . 121
Device Level AP GUI Interface . . . 123
Port Level AP GUI Interface . . . 124
Saving Changes . . . 125
Port Configuration . . . 126
Device Level . . . 126
Port Level . . . 127
Port Properties . . . 127
Associated Links . . . 129
Power Management . . . 130

Chapter 7.
User Management
Overview . . . 135
Browser GUI . . . 135
AP GUI . . . 135
Users . . . 137
Adding Users . . . 137
Modifying User Accounts . . . 141
Deleting User Accounts . . . 141
Groups . . . 142
Creating Groups . . . 142
Modifying Groups . . . 144
Deleting Groups . . . 144
Users and Groups . . . 145
Assigning Users to a Group From the User's Notebook . . . 145
Removing Users From a Group From the User's Notebook . . . 146
Assigning Users to a Group From the Group's Notebook . . . 147
Removing Users From a Group From the Group's Notebook . . . 148
Device Assignment . . . 149
Assigning Device Permissions From the User's Notebook . . . 149
Filters . . . 151
Assigning Device Permissions From the Groups' Notebook . . . 152

Chapter 8.
Device Management
KVM Devices . . . 153
Device Information . . . 153
General . . . 154
Environment . . . 154
Operating Mode . . . 155
Network . . . 157

IP Installer 158
Service Ports 158
NIC Settings 159
Network Transfer Rate 161
Finishing Up 161
ANMS 162
Event Destination 162
Authentication 165
CC Management Settings 168
SNMP Agent 169
OOBC 170
Enable Dial Back 171
Enable Dial Out 171
Security 173
Login Failures 173
Filter 174
Login String 177
Account Policy 178
Encryption 179
Mode 180
Private Certificate 181
Certificate Signing Request 182
Date/Time 184
Time Zone 184
Date 185
Network Time 185
PON Devices 186
Configuration Page 186
Outlet Configuration 187
Blade Servers 188
Configuration Page 188
Blade Server Setup 189
Adding a Blade Server 189
Modifying / Deleting a Blade Server 190
Web Access 190

Chapter 9.
Log
Overview 191
Browser GUI 191
AP GUI 191
Log Information 192
Filter 192
Log Notification Settings 194

Chapter 10.
Maintenance
Overview 195
Browser GUI 195
AP GUI 195
Main Firmware Upgrade 196

Firmware Upgrade Recovery 197
Upgrade Adapters. 198
Browser GUI 198
AP GUI 198
Upgrade Adapters 199
Adapter Firmware Info. 200
Browser GUI 200
AP GUI 200
Display Information 201
Update Adapter Display Info 201
Adapter Firmware Upgrade Recovery 202
Backup/Restore 203
Backup 203
Restore 204
Terminal 205
Restore Values 206
Clear Port Names:. 206
Restore Default Values: 206
Reset on exit: 206

Chapter 11.
Download
Overview. 207

Chapter 12.
Port Operation
Overview. 209
Connecting to a Port 210
The Port Toolbar. 211
The Toolbar Icons 212
Toolbar Hotkey Port Switching 213
Auto Scanning 213
Skip Mode 214
Recalling the Port Access Page 215
GUI Hotkey Summary Table 215
Panel Array Mode 216
Panel Array Toolbar 217
Multiuser Operation 218
Users and Buses. 219

Chapter 13.
The Log Server
Installation. 221
Starting Up 222
The Menu Bar 223
Configure. 223
Events 224
Search: 224
Maintenance:. 225
Options 226
Help. 226

The Log Server Main Screen 227
Overview 227
The List Panel 228
The Event Panel 228

Appendix

Safety Instructions. 229
General 229
Rack Mounting 231
Consignes de sécurité. 232
Général 232
Montage sur bâti 235
Technical Support 236
International. 236
North America 236
Specifications 237
KN4164V / KN8132V / KN8164V 237
Troubleshooting 239
General Operation 239
Mouse Problems 241
Virtual Media 243
Web Browser 243
The WinClient ActiveX Viewer and the WinClient AP 244
The Java Applet and Java Client AP 245
Sun Systems 246
Mac Systems 246
Redhat Systems 247
The Log Server 247
Panel Array Mode 247
IP Address Determination 250
The Local Console 250
IP Installer 250
Browser 251
IPv6 252
Link Local IPv6 Address 252
IPv6 Stateless Autoconfiguration 253
Port Forwarding. 254
Keyboard Emulation 255
Mac Keyboard 255
Sun Keyboard 256
PPP Modem Operation 257
Basic Setup 257
Connection Setup Example (Windows XP) 258
KA7140 Configuration and Operation 259
Configuration 259
Operation. 260
KA7140 Pin Assignments 261
Internal Serial Interface Configuration. 262
Navigation 262
Operation. 263
Switch Level Configuration 263

Port Level Configuration 264
Additional Mouse Synchronization Procedures 265
Windows:. 265
Sun / Linux 266
Additional Video Resolution Procedures 267
Trusted Certificates. 268
Overview 268
Installing the Certificate. 269
Certificate Trusted. 270
Mismatch Considerations 271
Self-Signed Private Certificates 272
Examples 272
Importing the Files. 272
Fan Location and Speed Information 273
Fan Location 273
Clear Login Information 274
Factory Default Settings 275
Serial Adapter Pin Assignments 275
Supported KVM Switches 276
Supported Power Over the Net™ Units 276
Supported Power Distribution Units 276
Virtual Media Support 277
WinClient ActiveX Viewer / WinClient AP 277
Java Client Viewer / Java Client AP 277
Limited Warranty. 278

About This Manual

This User Manual is provided to help you get the most from your KVM over IP switch system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Overview

Chapter 1, *Introduction***,** introduces you to the KVM over IP switch. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, *Hardware Setup***,** provides step-by-step instructions for setting up your installation, and explains some basic operation procedures.

Chapter 3, *Super Administrator Setup***,** explains the procedures that the super administrator employs to set up the KN8164V / KN8132V / KN4164V network environment, and change the default username and password.

Chapter 4, *Logging In***,** describes how to log in to the KVM over IP switch with each of the available access methods: from a local console; an Internet browser; a stand-alone Windows application (AP) program; and a stand-alone Java application (AP) program.

Chapter 5, *The User Interface***,** describes the layout and explains the components of the KVM over IP switch user interface.

Chapter 6, *Port Access***,** describes the Port Access page and how to configure the options it provides regarding port and power outlet manipulation.

Chapter 7, *User Management***,** shows super administrators and administrators how to create, modify, and delete users and groups, and assign attributes to them.

Chapter 8, *Device Management***,** shows super administrators how to configure and control overall KVM over IP switch operations.

Chapter 10, *Maintenance***,** explains how to upgrade the KVM over IP switch firmware, as well as the firmware of the KVM Adapter Cables used to connect its ports to the installed devices.

Chapter 11, *Download***,** describes how to download stand-alone AP versions of the Win Client, the Java Client, the Log Server, and Power Over the Net (PON) programs.

Chapter 12, *Port Operation***,** provides detailed information on accessing and operating the devices connected to the KVM over IP switch's ports.

Chapter 13, *The Log Server***,** explains how to install and configure the Log Server.

An Appendix, at the end of the manual provides technical and troubleshooting information.

Conventions

This manual uses the following conventions:

`Monospaced`	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
→	Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
	Indicates critical information.

Terminology

Throughout the manual we make reference to the terms *Local* and *Remote* in regard to the operators and equipment deployed in a KVM over IP switch installation. Depending on the point of view, users and servers can be considered *Local* under some circumstances, and *Remote* under others:

- Switch's Point of View
  - Remote users – We refer to a user as a *Remote* user when we think of him as someone who logs into the switch over the net from a location that is *remote from the switch*.
  - Local Console – The keyboard mouse and monitor connected directly to the switch.
  - Servers – The servers attached to the switch via KVM Adapter Cables.
- User's Point of View
  - Local client users – We refer to a user as a *Local client user* when we think of him as sitting at his computer performing operations on the servers connected to the switch that is *remote from him*.
  - Remote servers – We refer to the servers as *Remote servers* when we think of them from the Local Client User's point of view – since, although they are locally attached to the switch, they are *remote from him*.

When we describe the overall system architecture we are usually speaking from the switch's point of view – in which case the users are considered remote. When we speak about operations users perform via the browser, viewers, and AP programs over the net, we are usually speaking from the user's point of view – in which case the switch and the servers connected to it are considered remote.

Product Information

For information about all ALTUSEN products and how they can help you connect without limits, visit ALTUSEN on the Web or contact an ALTUSEN Authorized Reseller. Visit ALTUSEN on the Web for a list of locations and telephone numbers:

International	http://www.aten.com
North America	http://www.aten-usa.com

This Page Intentionally Left Blank

Chapter 1
Introduction

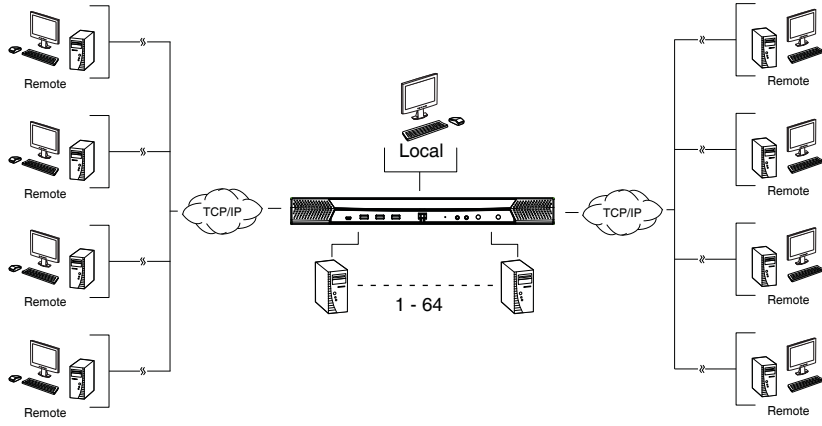
Overview

The KN4164V / KN8132V / KN8164V switches are IP-based KVM control units that allow both local and remote operators to monitor and access multiple servers from a single console. The KN4164V / KN8132V / KN8164V can control up to 32/64 servers, and by cascading compatible KVM switches, as many as 512 servers can be controlled on a complete two stage installation. These V-Series KVM over IP switches provide superior video quality – with resolutions up to 1920 x 1200, fast virtual media access to connected USB drives and supports IPS 140-2 level 1 security standards.

The switches in this series are differentiated according to the number of buses they support and the number of KVM ports they provide – as shown below:

Model	Bus Support	KVM Ports
KN4164V	1 Local; 4 Remote; 2U	64
KN8132V	1 Local; 8 Remote; 1U	32
KN8164V	1 Local; 8 Remote; 2U	64

Each bus permits a separate user session so that up to 5 (1 Local; 4 Remote) or nine (1 Local; 8 Remote) concurrent independent connections to the attached servers can take place. The diagram below shows how the KN8164V / KN8132V switches can be connected and accessed locally and remotely.



Since the switches use TCP/IP for their communications protocol, they can be accessed via their IP addresses from anywhere on the LAN, WAN, or Internet – whether the connecting computer is located down the hall, down the street, or half-way around the world. Remote operators can log in via their browser or make use of stand-alone Windows or Java GUI applications. Java allows the switches to work with JRE (Java Runtime Environment) enabled operating systems – ensuring multi-platform operability.

The client software allows operators to exchange keyboard, video and mouse signals with the servers attached to the switches just as if they were present locally and working on the equipment directly.

Up to 32 users can share the switch's buses. A *Message Board* feature allows them to communicate with each other to facilitate port sharing.

Administrators can handle a multitude of maintenance tasks with ease – from installing and running GUI applications, to BIOS level troubleshooting, routine monitoring, concurrent maintenance, system administration, rebooting and even pre-boot functions.

Local console operation is easily accomplished by entering *hotkey* combinations from the keyboard with a full screen GUI display.

Monitoring the installation's activities couldn't be easier. A convenient *Auto Scan* feature permits automatic switching from port to port at user-specified intervals, while the *Panel Array Mode* can display the video output of up to 42 servers at the same time.

The switches feature RJ-45 connectors allowing them to use CAT 5e cable to link to the servers. This space-saving innovation means that a full 32 or 64 port switch can be conveniently installed in a 2U system rack, and the installation can take advantage of the internal network wiring built into most modern commercial buildings.

Setup is fast and easy; plugging cables into their appropriate ports is all that is entailed. Because the switch intercepts keyboard input directly, there is no need to get involved in complex software installation routines, or to be concerned with incompatibility problems.

Since the firmware is upgradeable over the Net, you can stay current with the latest functionality improvements simply by downloading firmware updates from our website as they become available.

With its powerful security features, the KVM over IP switch provides the fastest, most reliable, most cost effective way to remotely access and manage widely distributed multiple server installations.

KVM over IP switches have an *Adapter ID* function that stores port information like the adapter ID, OS, keyboard language, adapter name, operation modes and more, so that when you move a KVM Adapter Cable from one port to another, the switch recognizes the same adapter cable at the new location. Also, for greater ease of use when moving the adapter cable to another switch, the adapter ID, OS, keyboard language, adapter name, and operation modes of the port stay with the adapter.

The KN4164V / KN8132V / KN8164V supports advanced virtual media functions, such as a higher transmission speed, mapping USB DVD/CD/hard drives; and other storage media to a server. Virtual media support allows you to conduct file transfers, installs applications and OS patches, and perform diagnostics remotely. You can upgrade your entire installation from a single remote console located anywhere in the world.

The KN8 models offer dual power supplies so that if one of the power supplies fails, the second power supply automatically takes over. In addition to supporting dual power, they guard against power failure from your server room outlets. If your server room has more than one power source, connecting the power supplies to different power sources is a wise choice. If one of the server room power supplies loses power, the switch will automatically adjust the power it draws from the second source to keep functioning.

The KN4164V / KN8132V / KN8164V models support temperature sensors that can control internal fans. The sensors regulate the fans so that they run at optimum speed depending on the server room temperature – throttling down when necessary, to use energy more efficiently and prolong the life of both the fans and the switch.

The KN4164V / KN8132V / KN8164V models are also audio enabled. Microphone and speakers are supported on the Local Console for the servers; speakers are supported on the remote users' computers.

Features

Hardware

- High port density – RJ-45 connectors and Cat 5e/6 cable for up to 32 ports (KN8132V) in a 1 U housing or 64 ports (KN4164V / KN8164V) in a 2U housing
- Eight separate buses for remote KVM over IP access
- Two 10/100/1000 Mbps NICs for redundant LAN or two IP operation
- Supports PS/2, USB, Sun Legacy (13W3) and serial (RS-232) connectivity
- Local console provides USB keyboard and mouse support
- Supports multi-platform server environments: Windows, Mac, Sun, Linux and VT100 based serial devices
- High video resolution – up to 1920 x 1200 @ 60Hz – 24 bit color depth for the local console; up to 1920 x 1200 @ 60Hz with 24 bit color depth for remote sessions, at up to 50 m
- Monitor and control up to 32 or 64 computers on a single level, or control up to 512 computers in a cascade*

* Cascade-compatible KVM Switches include the following: CS9134, CS9138, CS88A, KH1508, KH1516, KH1508A, and KH1516A

Management

- Up to 64 user accounts – up to 32 users simultaneously share the control
- End session feature – administrators can terminate running sessions
- Event logging and Windows-based Log Server support
- Critical system event notification via SMTP email; SNMP trap and Syslog support
- Customizable event notification
- Firmware upgradable
- Out-of-Band Access-Modem dial-in/dial out/dial back support
- Adapter ID Function: Stores port information allowing administrators to relocate the servers to different ports, without having to re-configure the adapters and switches.
- Port Share Mode allows multiple users to gain access to a server simultaneously

- Integration with ALTUSEN CC2000 Management software
- Power Association enables the switch's KVM ports to be associated with a PDU's power outlets for remote power management of the servers from the switch's interface
- Manage browser access (Browser, http, https)
- IPv6 capable

Easy-to-Use Interface

- Local Console, browser based, and AP GUIs offer a unified multi-language interface to minimize the user training time and increase productivity
- Multiplatform client support (Windows, Mac OS X, Linux, Sun)
- Multi-browser support: Internet Explorer, Chrome, Firefox, Safari, Opera, Mozilla, Netscape
- Browser-based UI in pure Web technology allows administrators to perform administrative tasks without pre-installed Java software package required
- Launch multiple Virtual Remote Desktops to control multiple servers from the same login session
- Magic Panel
- Full-screen or sizable and scalable Virtual Remote Desktop
- Panel Array Mode available to both local console and remote access users
- Keyboard/Mouse Broadcast – keyboard and mouse inputs can be duplicated on all the attached servers
- Video syncing with the local console – local console monitor's EDID information stored on the KVM Adapter Cables for display resolution optimization

Advanced Security

- Remote authentication support: RADIUS, LDAP, LDAPS, and MS Active Directory
- Supports SSL 128-bit data encryption and RSA 2048-bit certificates to secure user logins from browsers
- Flexible encryption design allows users to choose any combination of 56-bit DES, 168-bit 3DES, 256-bit AES, 128-bit RC4, or Random for independent KB/Mouse, video, and virtual media data encryption
- Support for IP/MAC Filter

- Configurable user and group permissions for server access and control
- Automated CSR creation utility and third party CA certificate authentication

Virtual Media

- Virtual media enables file applications, OS patching, software installation and diagnostic testing
- Works with USB enabled servers at the operating system and BIOS level
- Supports DVD/CD drives, USB mass storage devices, PC hard drives and ISO images
- Supports Smart Card Readers on computers connected with KA7166, KA7168, KA7169, KA7177 Adapter Cables

Virtual Remote Desktop

- Video quality can be adjusted to optimize data transfer speed; monochrome color depth setting, threshold and noise settings for compression of the data bandwidth in low bandwidth situations
- High-performance graphics for the best image quality
- Full screen video display or scalable video display
- Message Board for communication among remote users
- Mouse DynaSync™ automatically synchronizes the local and remote mouse movements
- Exit Macros support
- On-screen keyboard with multilanguage support
- BIOS-level access

KN8 V-Series Exclusive

- Advanced FPGA graphics processor for improved video quality
- Higher transmission speed for virtual media devices
- 8 separate buses for remote KVM over IP access
- Supports FIPS 140-2 level 1 security standards

System Requirements

Remote User Computers

Remote user computers (also referred to as client computers) are the ones the users log into the switch with from remote locations over the Internet (see *Terminology*, page xvii). The following equipment must be installed on these computers:

- For best results we recommend computers with at least a P III 1 GHz processor, with their screen resolution set to 1024 x 768.
- IE8 or above web browser
- Browsers must support 128 bit SSL encryption.
- For best results, a network transfer speed of at least 512kbps is recommended.
- For the browser-based WinClient ActiveX Viewer, DirectX 8 must be present, and at least 150MB of memory must be available after installation.
- For the browser-based Java Client Viewer the latest version of the Java Runtime Environment (JRE) must be installed, and at least 205MB of memory must be available after installation.
- For the Windows Client AP, DirectX 8 must be present, and at least 90MB of memory must be available after installation.
- For the Java Client AP, the latest version of the Java Runtime Environment (JRE) must be installed, and at least 145MB of memory must be available after installation.
- For the *Log Server*, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.

Servers

Servers are the computers connected to the switch via KVM Adapter Cables (see *Terminology*, page xvii). The following equipment must be installed on these servers:

- A VGA, SVGA or multisync port
- For USB KVM Adapter Cable Connections: a Type A USB port and USB host controller
- For PS/2 KVM Adapter Cable Connections: 6-pin Mini-DIN keyboard and mouse ports

KVM Adapter Cables

- Cat 5e (or higher) cable is required to connect the KVM over IP switch to the KVM Adapter Cables (see page 25).
- The following KVM Adapter Cables are required for use with the KVM over IP switch:

Function	Module
Connect to devices with PS/2 ports	KA7120
Connect to devices with USB ports (All platforms – PC, Mac, Sun)	KA7170
Connect to Sun Legacy Computers	KA7130
Connect to serial based devices	KA9140 / KA7140
For USB computers – DVI output, Virtual Media and Smart Card Reader support	KA7166
For USB computers – HDMI output, Virtual Media and Smart Card Reader support	KA7168
For USB computers – DisplayPort output, Virtual Media and Smart Card Reader support	KA7169
Connect to devices with USB ports and virtual media support	KA7175
Connect to devices with USB ports, virtual media and audio support	KA7176
Connect to devices with USB ports, with virtual media, smart card reader support	KA7177

Note: If you use Adapter Cables purchased prior to your switch purchase, you may have to upgrade the Adapter's firmware. (see page 198).

Operating Systems

- Supported operating systems for remote user computers include Windows 2000 and higher, and those capable of running the Java Runtime Environment (JRE) 6, Update 3, or higher (Linux, Mac, Sun, etc.).
- Supported operating systems for the servers connected to the switch's ports are shown in the table, below:

OS		Version
Windows		2000 and higher
Linux	RedHat	7.1 and higher
	Fedora	Core 2 and higher
	SuSE	9.0 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	4.2 and higher
	Sun	Solaris 8 and higher
Novell	Netware	5.0 and higher
Mac		OS 9 and higher*
DOS		6.2 and higher

Browsers

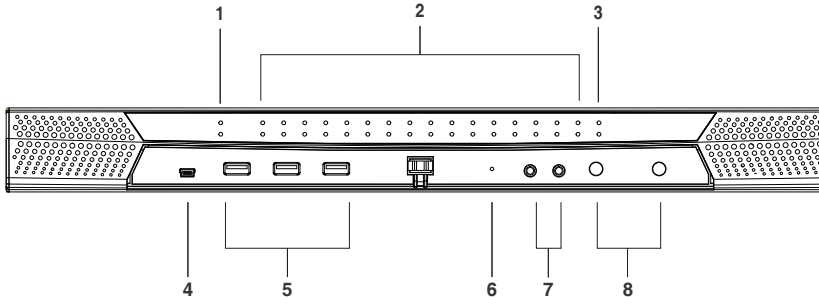
Supported browsers for users that log into the KVM over IP switch include the following:

Browser		Version
IE		8 and higher
Chrome		8.0 and higher
Firefox	Windows	3.5 and higher
	Linux	3.0 and higher
Safari	Windows	4.0 and higher
	Mac	3.1 and higher
Opera		10.0 and higher
Mozilla	Windows	1.7 and higher
	SUN	1.7 and higher
Netscape		9.0 and higher

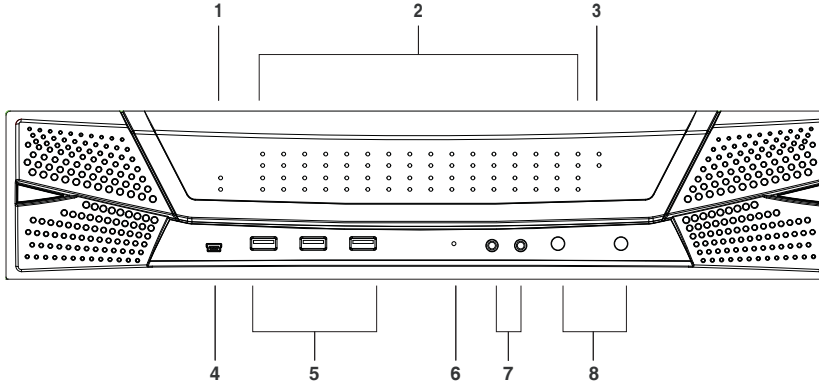
***** See *Mac Systems*, page 246, for further information.

Components

KN8132V Front View



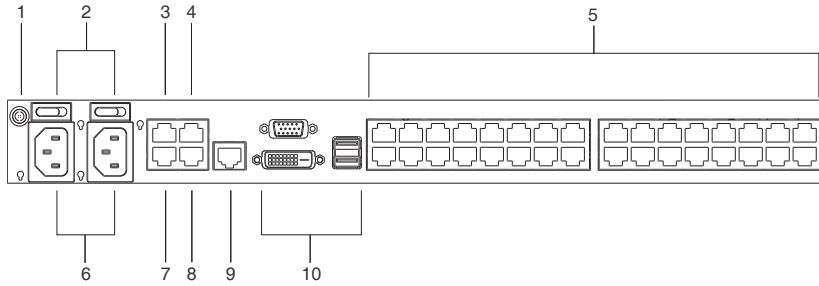
KN8164V / KN4164V Front View



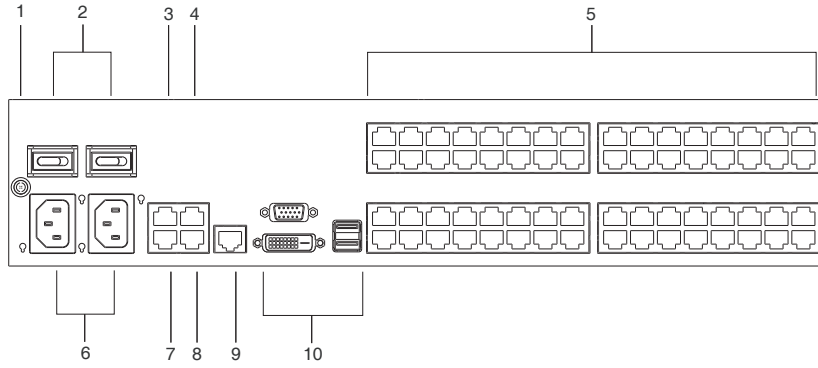
No.	Component	Description
1	Power LED	Lights BLUE when the unit is powered on and indicates which of the two power sources are available.
2	Port LEDs	The Port LEDs provide status information about their corresponding KVM Ports. ◆ GREEN: The computer attached to the port is On Line. ◆ RED: The computer attached to the port is Selected (has KVM focus). ◆ GREEN + RED (ORANGE): The computer attached to the port is On Line and Selected. The LEDs are steady under normal conditions. A LED will flash at half second intervals, however, when its corresponding port is accessed under Auto Scan Mode or Skip Mode (see pages 213 and 214).
3	LAN LEDs	Primary and Secondary 10/100/1000 Mbps LAN LEDs. ◆ RED: 10 Mbps ◆ RED + GREEN (ORANGE): 100 Mbps ◆ GREEN: 1000 Mbps ◆ Flashes to indicate that the switch is being accessed over the Net.
4	Laptop USB Console Port	A dedicated USB port for directly connecting a laptop to the switch for easy console operation.
5	USB Ports	A USB keyboard and mouse can plug in here. This can either be in place of, or in addition to, plugging a keyboard and mouse into the ports on the rear panel. This port can also be used to connect USB storage peripherals (CD/DVD, HD, flash drives, etc.) on V series switches.
6	Reset Switch	**Note:** This switch is recessed and must be pushed with a small object such as the end of a paper clip, or a ballpoint pen. ◆ Pressing and releasing this switch when the unit is running performs a system reset. ◆ Pressing and holding this switch in for more than three seconds when the unit is running resets its configuration to the factory default settings. **Note:** This does not clear User Account information. See *Clear Login Information*, page 274, for information on clearing user account information. ◆ Pressing and holding this switch while powering on the switch returns the unit to its factory default firmware level, rather than the firmware version that the switch has been upgraded to. This allows you to recover from a failed firmware upgrade and gives you the opportunity to try upgrading the firmware again. **Note:** This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable.
7	Audio Ports	Speakers and microphone plug in here.

No.	Component	Description
8	Port Switching Buttons	◆ Press **PORT DOWN** to manually switch from the current port to the previous port on the installation. ◆ Press **PORT UP** to manually switch from the current port to the next port on the installation.

KN8132V Rear View



KN8164V / KN4164V Rear View



No.	Component	Description
1	Grounding Terminal	The wire used to ground the unit connects here.
2	Power Switch	These standard slide switches power the unit on and off.
3	Secondary LAN Port	The cable that connects the unit to the backup network interface (10/100/1000 Mbps) plugs in here.
4	PON Port	This connector is provided for a Power over the Net™ (PON) unit which allows servers attached to the KVM over IP switch to be booted remotely over the net. See *Single Stage Installation*, page 25, step 6 for installation details. Contact your dealer for more information regarding PON units.
5	KVM Ports	The Cat 5e cables that link the unit to the KVM Adapter Cables (which connect to the servers), plug in here.
6	Power Sockets	The power cable(s) plugs in here. The left power socket corresponds to the left power switch, and the right power socket corresponds to the right power switch.
7	Primary LAN Port	The cable that connects the unit to the primary network interface (10/100/1000 Mbps) plugs in here.
8	Modem Port	For dial in connection should the unit be unavailable over the network. See *Single Stage Installation*, page 25, step 7 for installation details.
9	Remote Console Port	This port is reserved and will be available for use with future upgrades as a remote console port.
10	Local Console Port(s)	The unit can be accessed via a local console as well as over the Net. The local console devices (USB keyboard, USB mouse, DVI-D or VGA monitor) plug in here.

Chapter 2
Hardware Setup

Overview

For convenience and flexibility that allows USB interfaces, as well as multiple platforms, the KVM over IP switch design utilizes KVM Adapter Cables, that serve as intermediaries between the switch and the connected devices (see *Adapter Cable Connection Diagram*, page 28 for details).

A separate KVM Adapter Cable is required for each server or device connection. The model numbers of the Adapters are given in the *KVM Adapter Cables* section, page 8.

Before You Begin

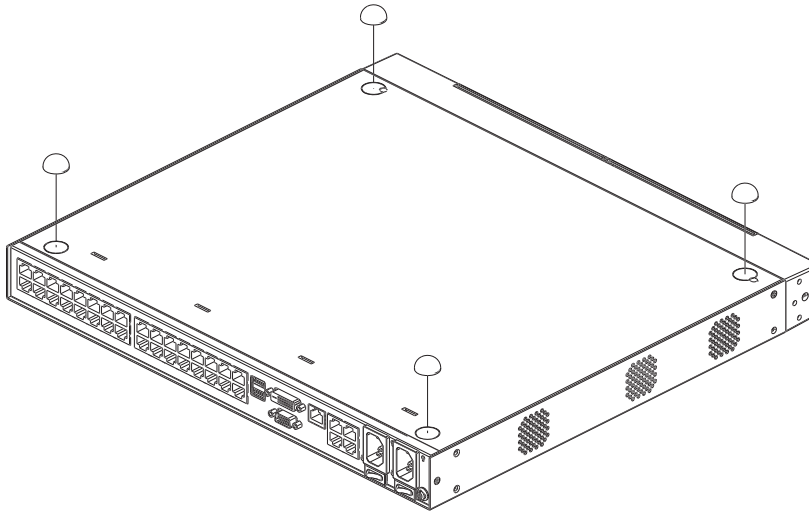
1. Important safety information regarding the placement and grounding of this device is provided on page 229 and onwards. Please review it before proceeding.
2. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords

Stacking and Rack Mounting

The KVM over IP switch can be stacked on the desktop or rack mounted in a variety of ways. The following sections take you through the procedures for each method.

Stacking

The KVM over IP switch can be placed on any appropriate level surface that can safely support its weight plus the weight of its attached cables. To place the switch, or to stack units if you are daisy-chaining them, remove the backing material from the bottom of the rubber feet that came with your package, and stick them onto the switch's bottom panel at the corners, as shown in the diagram, below:



Note: To ensure adequate ventilation, allow at least 5.1 cm on each side, and 12.7 cm behind the unit for power cord and cable clearance.

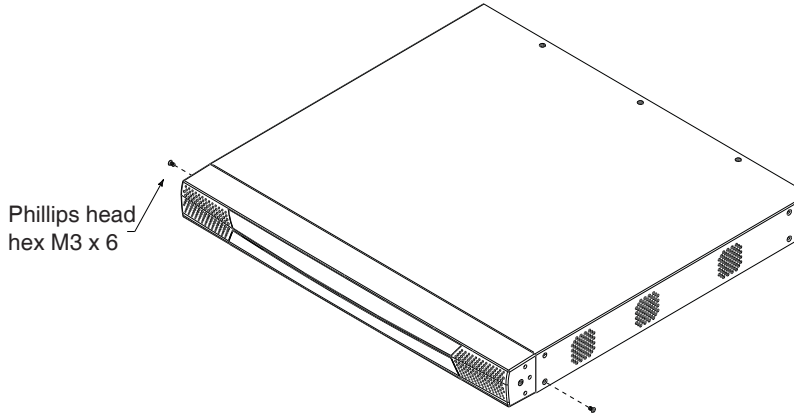
KN8132V Rack Mounting

The KN8132V can be mounted in a 19" (1U) rack. The mounting brackets can screw into either the front or the back of the unit so that it can attach to the front or the back of the rack.

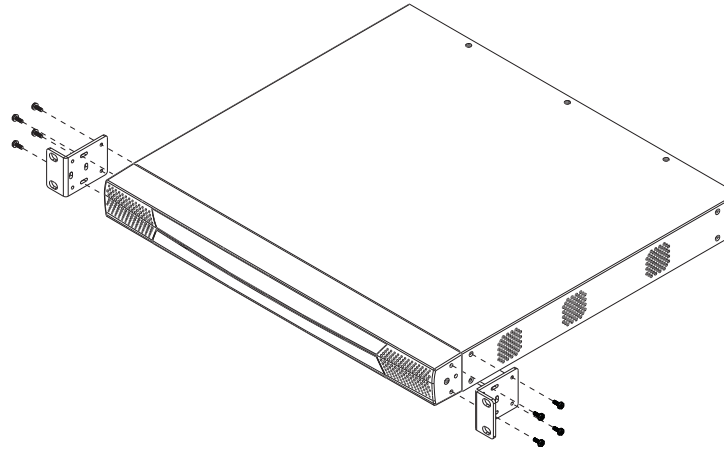
Rack Mounting - Front

To mount the unit at the front of the rack, do the following:

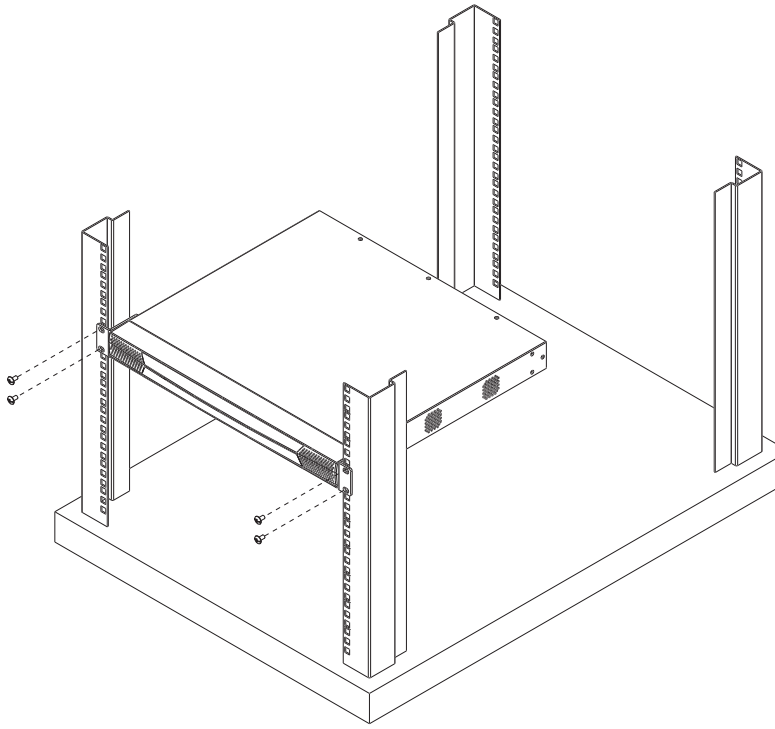
1. Remove the screws at the front of the unit.



2. Use the M3 x 8 Phillips head hex screws supplied with the rack mount kit to screw the rack mounting brackets into the front of the unit.



3. Position the device in the front of the rack and align the holes in the mounting brackets with the holes in the rack.
4. Screw the mounting brackets to the rack.

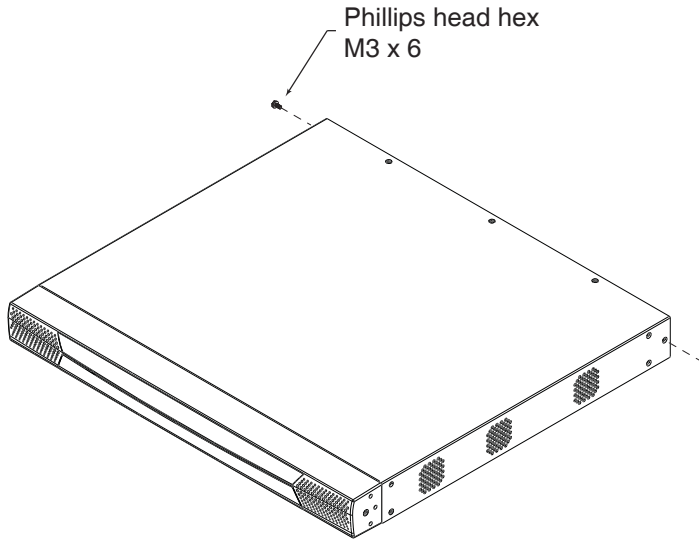


Note: Cage nuts are provided for racks that are not pre-threaded.

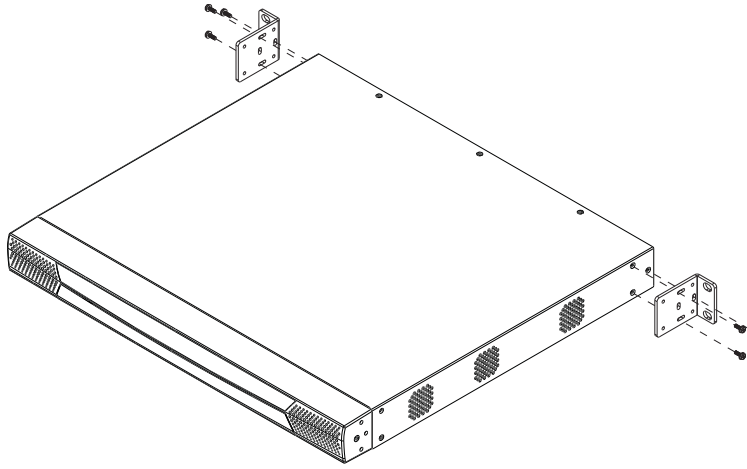
Rack Mounting - Rear

To mount the unit at the rear of the rack, do the following:

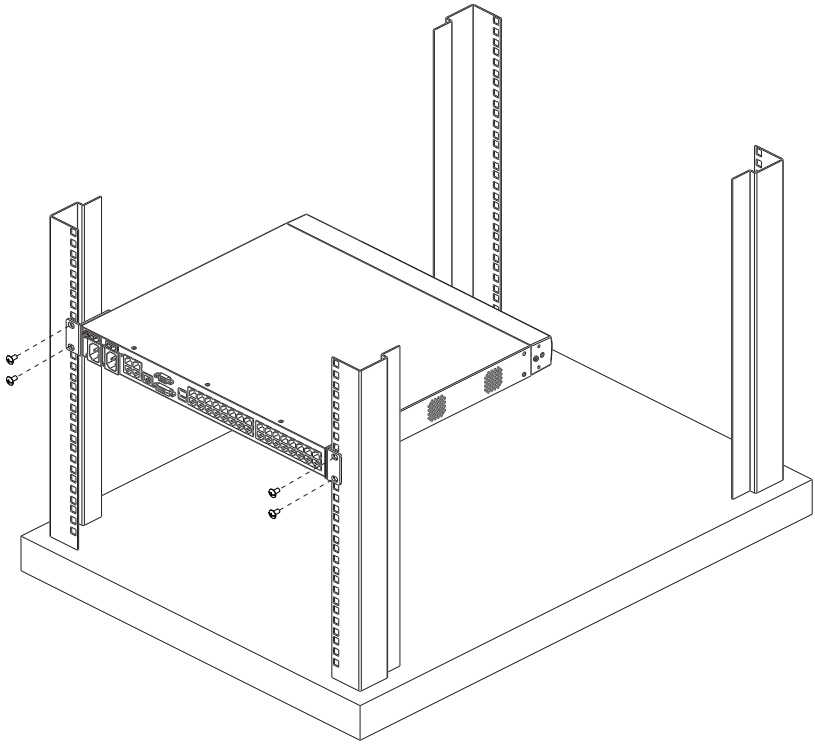
1. Remove the two screws at the rear of the unit.



2. Use the M3 x 8 Phillips head hex screws supplied with the rack mounting kit to screw the rack mounting brackets into the rear of the unit.



3. Position the device in the rack and align the holes in the mounting brackets with the holes in the rack.
4. Screw the mounting brackets to the rear of the rack.



Note: Cage nuts are provided for racks that are not prethreaded.

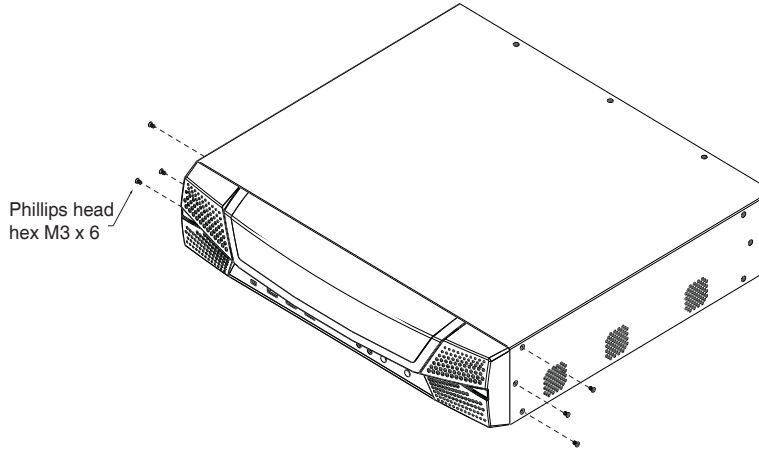
KN8164V / KN4164V Rack Mounting

The KN8164V / KN4164V can be mounted in a 19" (2U) rack. The mounting brackets can screw into either the front or the back of the unit so that it can attach to the front or the back of the rack.

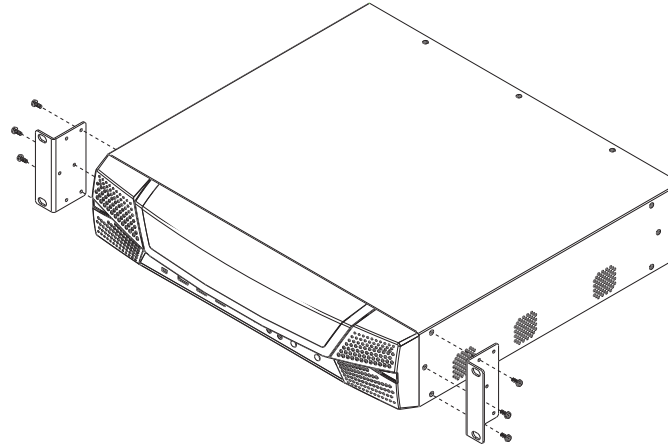
Rack Mounting - Front

To mount the unit at the front of the rack, do the following:

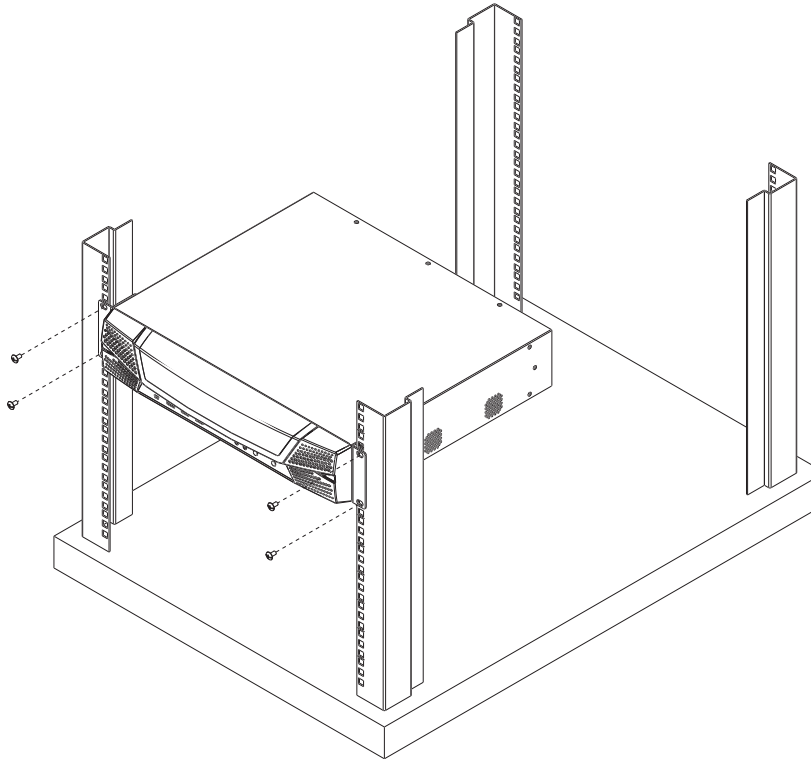
1. Remove the six screws at the front of the unit.



2. Use the M3 x 8 Phillips head hex screws supplied with the rack mount kit to screw the rack mounting brackets into the front of the unit.



3. Position the device in the front of the rack and align the holes in the mounting brackets with the holes in the rack.
4. Screw the mounting brackets to the rack.

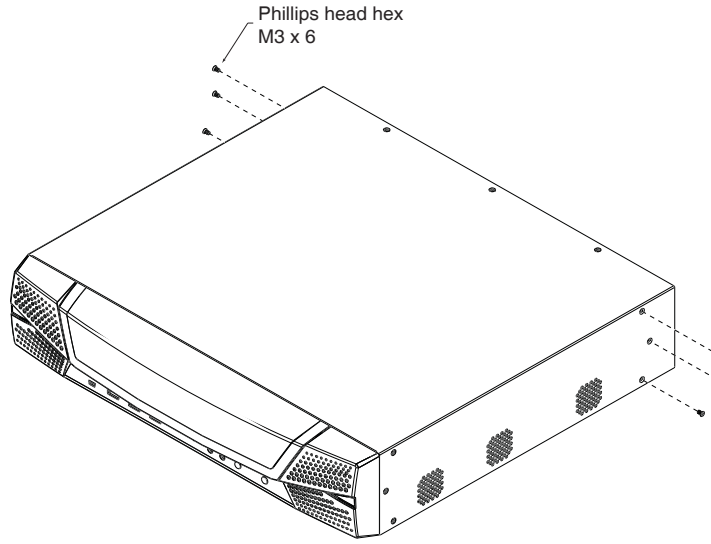


Note: Cage nuts are provided for racks that are not pre-threaded.

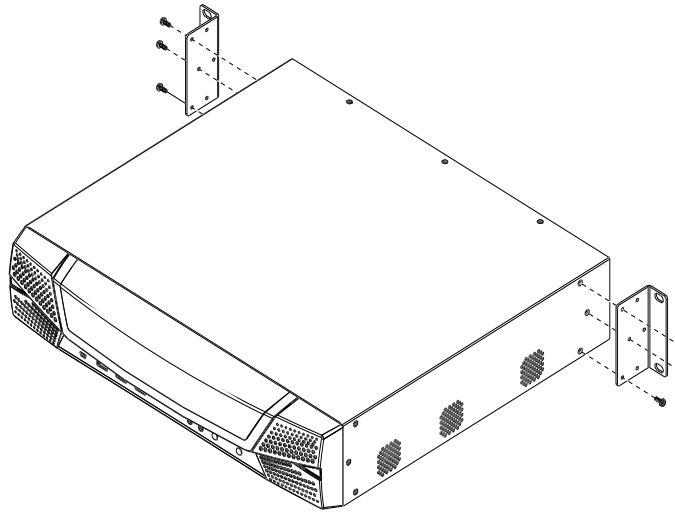
Rack Mounting - Rear

To mount the unit at the rear of the rack, do the following:

1. Remove the six screws at the rear of the unit.

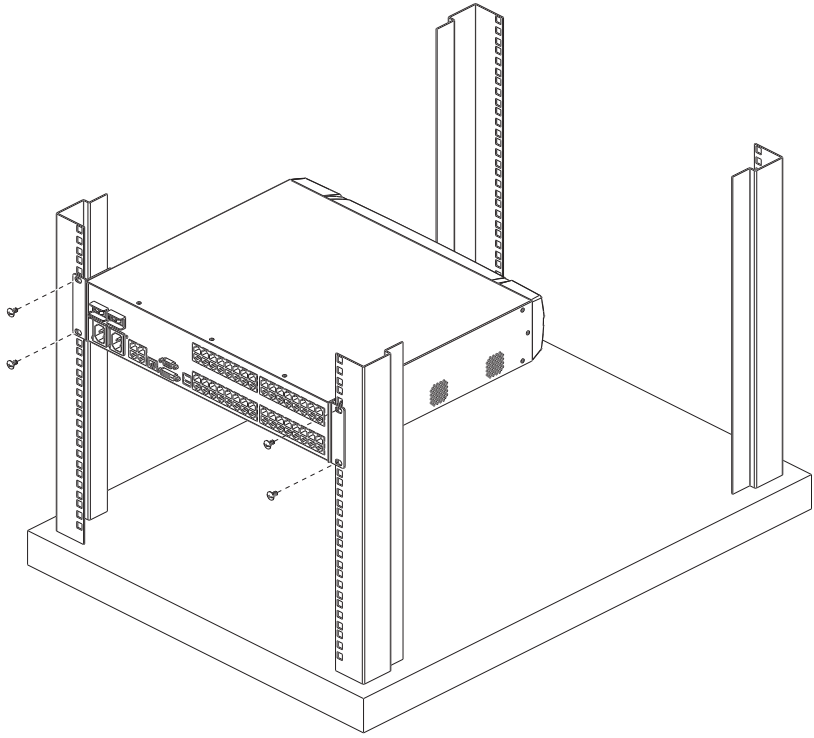


2. Use the M3 x 8 Phillips head hex screws supplied with the rack mounting kit to screw the rack mounting brackets into the rear of the unit.



3. Position the device in the rack and align the holes in the mounting brackets with the holes in the rack.

4. Screw the mounting brackets to the rear of the rack.



Note: Cage nuts are provided for racks that are not pre-threaded.

Single Stage Installation

In a single stage installation, no additional switches are cascaded from the original switch. To set up a single stage installation, refer to the installation diagrams starting on page 25 (the numbers in the diagram correspond with the numbers of the instruction steps), and do the following:

1. Plug your Local Console's keyboard, monitor, and mouse into the unit's Console Ports. Each port is color coded and marked with an appropriate icon.

   Note: 1. USB keyboards and mice can plug into the USB ports on the front panel, as well as into the ports in the console port section.

   2. The KVM over IP switch does not support distances that exceed 20m between itself and the local monitor.

2. Use Cat 5e cable to connect any available KVM port to a KVM Adapter Cable that is appropriate for the server you are installing (see the table on page 8 for details).

   Note: 1. If you are using a KA7120 or KA7130 Adapter Cable, refer to page 265 for mouse pointer synchronization information.

   2. If you are using a KA7140 Adapter Cable, refer to page 259 for setup and operation information.

   3. The distance between the switch and the KVM Adapter Cable must not exceed these lengths: KA7140: 300m; KA71xx: 50m.

3. Plug the connectors on the KVM Adapter Cable into the appropriate ports of the server you are installing. (See *Adapter Cable Connection Diagram*, page 28.)

4. Plug a cable from the LAN or WAN into the KVM over IP switch's primary network interface socket.

5. (Optional) Plug another cable from the LAN or WAN into the KVM over IP switch's backup (secondary) network interface socket.

6. (Optional) Use Cat 5e cable to connect the KVM over IP switch's PON port to an SA0142 Adapter. Connect the Adapter to the PON IN port of a Power Over the Net™ unit.

Note: 1. For Power Over the Net™ units and Power Distribution Units, go to Device Management/OOBC/Console Port Settings of the GUI and select a Baud Rate of 38400 bps.

2. Make sure the CC Management function is disabled for both the KN and PN.

3. The PON unit shown in the example is the PN0108. See *Supported Power Over the Net™ Units* and *Supported Power Distribution Units*, page 276, for a list of suitable units.

7. (Optional) Use Cat 5e cable to connect the KVM over IP switch's Modem port to an SA0142 Adapter. Connect the Adapter's serial connector to the modem's DB-9 port.

8. Ground the switch using proper grounding wire to connect the switch's grounding terminal to a suitable grounded object.

Note: Do not omit this step. Proper grounding helps to prevent damage to the unit from surges or static electricity.

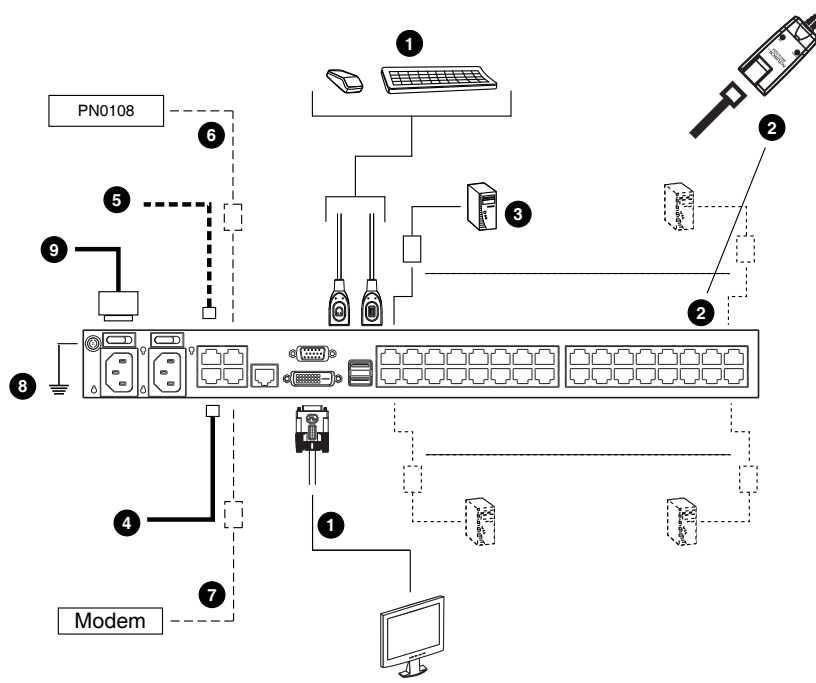
9. Plug the power cords supplied with your package into the switch's power socket, and then into an AC power source.

   When using a single power socket, be sure to turn on the correct power switch (see *Power Switch*, page 14). When using both power sockets, either of the power switches can be used to turn on the KVM switch. To enable dual power, turn on both power switches.

Note: If you are connecting the power to a UPS or an ALTUSEN PN9108/PN0108, be sure to use the utility power cords supplied with your package instead of standard power cords.

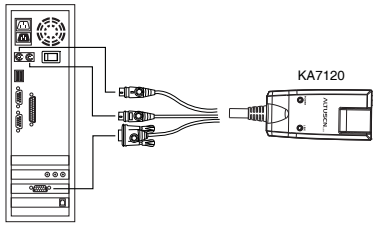
10. After the KVM over IP switch is cabled up you can turn on the power. After it is powered up, you can turn on the servers.

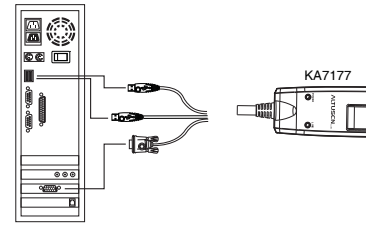
Single Stage Installation Diagram

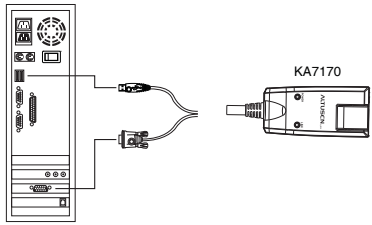


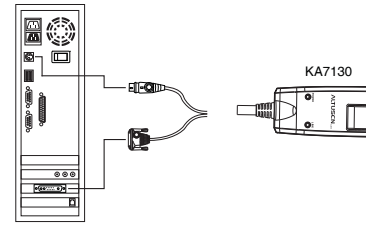
Note: The diagram above shows an installation with the KN8132V. Installing the KN8164V is same as the KN8132V and only differs in that it provides an additional 32 KVM ports.

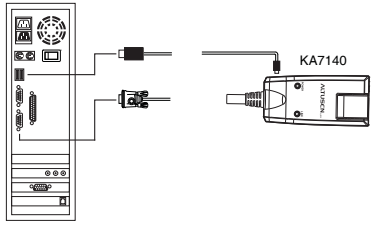
Adapter Cable Connection Diagram

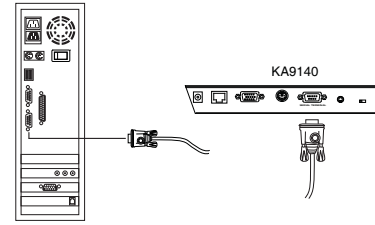


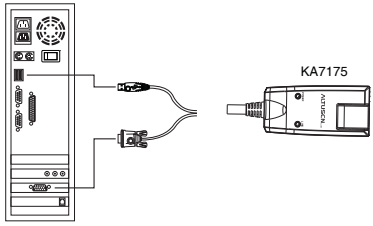


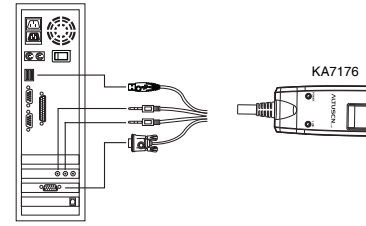




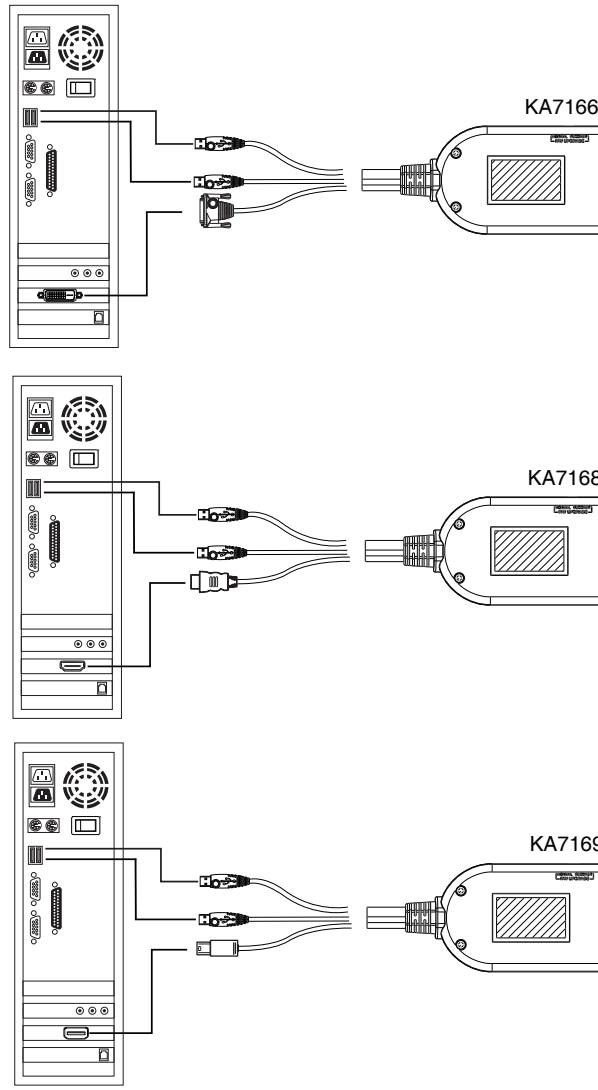








Adapter Cable Connection Diagram cont.



Two Stage Installation

To control even more servers, up to 32 additional KVM switches can be cascaded from the KVM ports of the original KVM over IP switch. As many as 512 servers can be controlled in a complete two stage installation.

In a cascaded installation, the KVM over IP switch is considered the *First Stage* unit, the cascaded switches are considered *Second Stage* units.

Note: The cascaded KVM switch shown in the example is the KH1516. See *Supported KVM Switches*, page 276, for a list of other switches.

To set up a two stage installation, refer to the diagram on page 31, and do the following:

1. Make sure that power to all the devices you will be connecting, including all preexisting devices on the installation, are properly grounded and have been turned off.
2. Use Cat 5e cable to connect any available KVM Port on the First Stage unit (the KVM over IP switch) to a KVM Adapter Cable (as described under *KVM Adapter Cables*, page 8).
3. Plug the adapter cable's KVM connectors to the Keyboard, Video, and Mouse Console ports of the Second Stage unit.

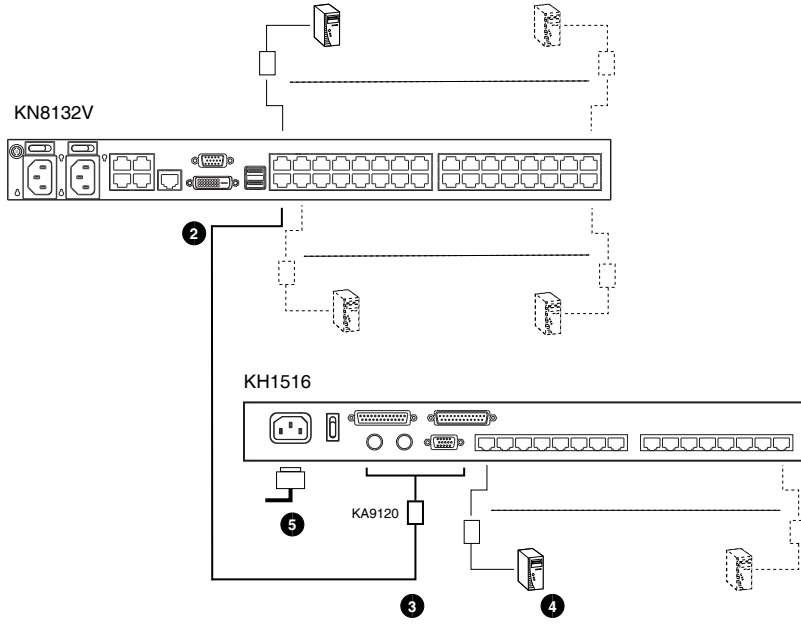
   Note: The distance between the *First Stage* unit and the *Second Stage* unit must not exceed 40m or 50m based on the KVM adapter cable used.

4. Use KVM cable sets (as described in the Cables section of the cascaded KVM switch's User Manual), to connect any available KVM port on the *Second Stage* unit to the Keyboard, Video, and Mouse ports of the servers you are installing.
5. Plug the power cord that came with the cascaded KVM switch into its Power Socket, and then into an AC power source.
6. Repeat these steps for any additional *Second Stage* units you wish to connect.
7. Power on the *Second Stage* unit(s), then power on the *First Stage* unit.
8. Turn on the power to all the servers.

   Note: The Power On sequence requires that all *Second Stage* switches be powered on first. After all *Second Stage* switches are powered on,

the *First Stage* switch can be powered on. After all the switches are powered on, the servers can be powered on.

Two Stage Installation Diagram



Note: The diagram above shows an installation with the KN8132V. Cascading the KN8164V or KN4164V is same as the KN8132V and only differs in that they provide an additional 32 KVM ports.

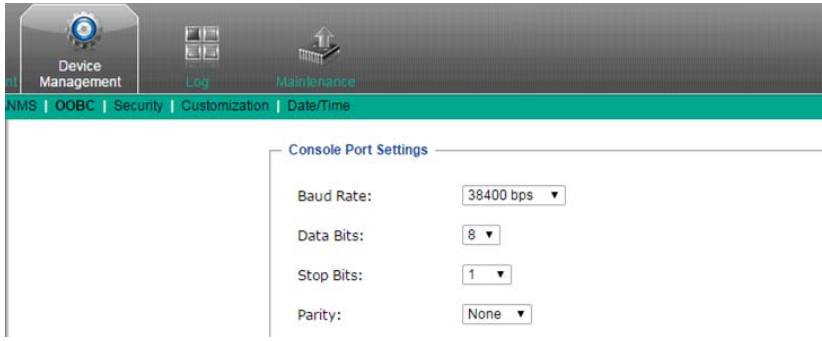
PDU Installation

ATEN PDU products are intelligent Power Distribution Units that offer outlet level control combined with remote access to give IT administrators the ability to power control devices attached to the unit from practically any location via a TCP/IP connection.

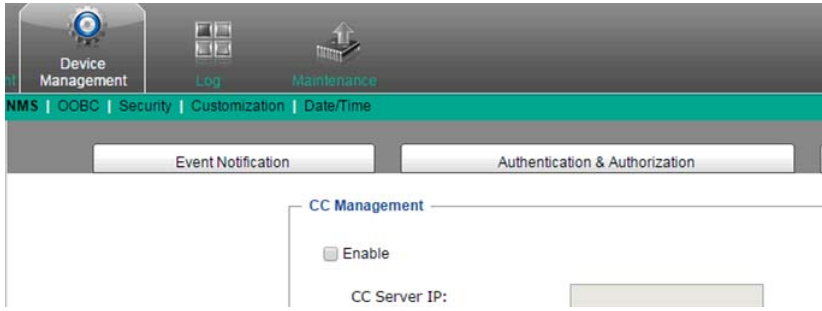
Note: The PDU GUI shown in the example is the PE9216r. See *Supported Power Distribution Units*, page 276, for a list of other PDUs.

To set up a PDU in conjunction with KVM over IP switches, refer to the images below and do the following:

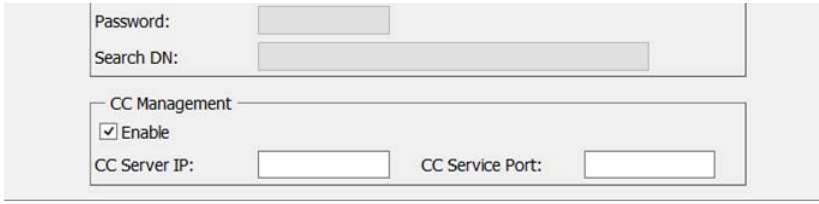
1. Connect both the KVM over IP Switch and the PDU to your Ethernet switch.
2. In the PDU's GUI, browse to Device Management, then to OOBC. In Console Port Settings, set the Baud Rate to 38400 bps.



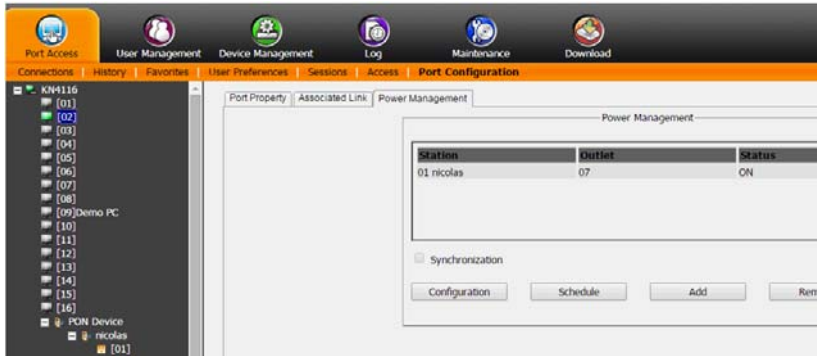
3. Still in Device Management, browse to ANMS. In CC Management, uncheck Enable.



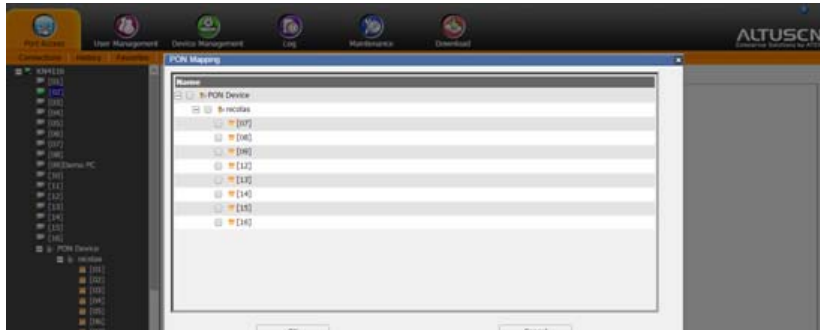
4. Next, connect the PDU (Console PON IN) directly to the KVM over IP switch (PON).
5. Following this, using the KVM over IP switch GUI, browse to Device Management, then to ANMS. In Authentication, uncheck CC Management.



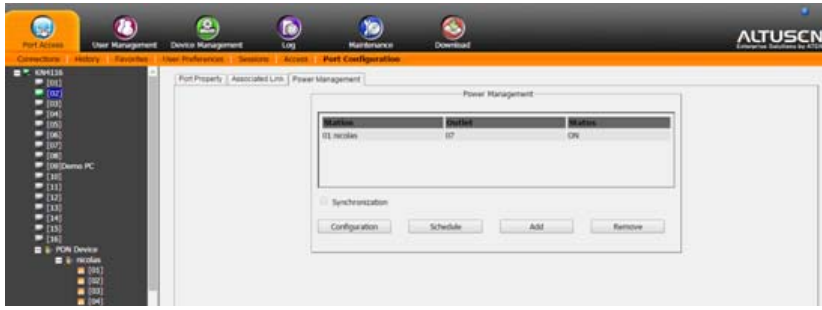
6. Finally, confirm that appropriate power management permission has been assigned. Browse to Port Access, then to Port Configuration. Select the relevant port number from the left tree menu.



Select Add (a power device).



The power outlet permission will then be assigned to the port you selected.



Hot Plugging

KVM over IP switches support hot plugging – components can be removed and added back into the installation by unplugging and replugging cables from the ports without the need to shut the unit down.

Note: If the server's Operating System does not support hot plugging, this function may not work properly.

The Adapter ID Function

Adapter Cable information (the Adapter ID, port name, OS, keyboard language, and access mode), is stored on the adapter. The switch's *Adapter ID* function takes this information and stores it along with the adapter cable's configuration information (access rights, etc.), in its database – so that when you move a server together with its adapter cable from one port to another, you don't have to reconfigure its settings – the Adapter ID function restores them at the new location. The only change is in the port number.

When moving the server and adapter cable to another switch, however, only the information that is stored on the adapter is retained. For the other settings you must either reconfigure them, or use the *Backup/Restore* function (see page 203) to restore them.

Since port settings are stored with the adapter, if you move a server to a new port without its original adapter; or if you connect a different server to the adapter, you must manually reconfigure the port settings for the new server. See *Sidebar Utilities*, page 98 for port configuration details.

Powering Off and Restarting

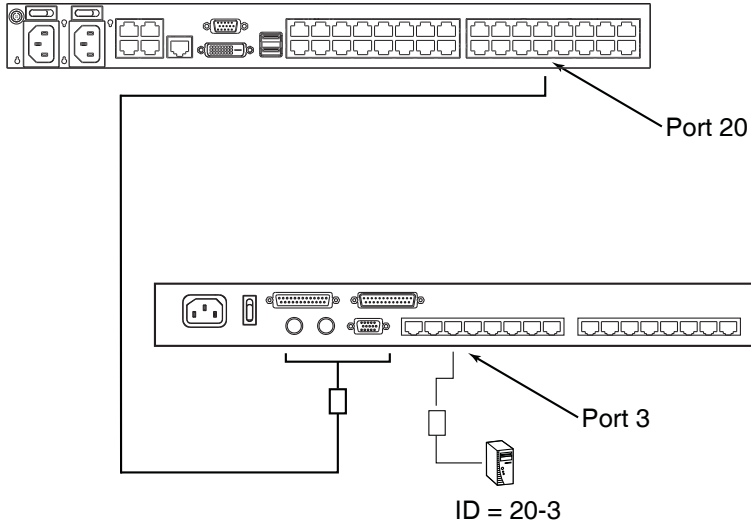
If it becomes necessary to power off the switch, or if the switch loses power and needs to be restarted, wait 30 seconds before powering it back on. The servers should not be affected by this, but if any of them should fail, simply restart them.

Port ID Numbering

Each server on the installation is assigned a unique Port ID. Its Port ID is a one or two segment number that is determined as follows:

- A server attached to a First Stage unit has a one segment Port ID (from 1–64) that corresponds to the KVM Port number that it is connected to.
- A server attached to a Second Stage unit has a two segment Port ID:
  - The second segment (from 1–16), represents the KVM Port number on the Second Stage unit that the server is connected to.
  - The first segment (from 1–64) represents the KVM Port number on the First Stage unit that the Second Stage unit links back to.

For example, a Port ID of 20 - 3 refers to a server that is connected to KVM Port 3 of a Second Stage unit that links back to KVM Port 20 of the First Stage unit:



Port Selection

Port selection is accomplished by means of the GUI. Port selection details are discussed in Chapter 6, *Port Access*.

Chapter 3
Super Administrator Setup

Overview

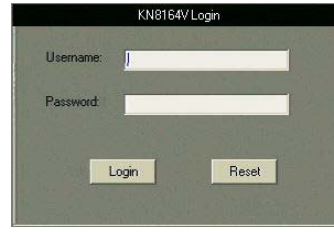
This chapter discusses the administrative procedures that the Super Administrator performs to get the KVM over IP switch set up for the first time.

First Time Setup

Once the KVM over IP switch has been cabled up, the Super Administrator needs to set the unit up for user operation. This involves setting the network parameters, and changing the default Super Administrator login. The most convenient way to do this for the first time is from the local console.

Note: For remote methods of setting up the network, see *IP Address Determination*, page 250.

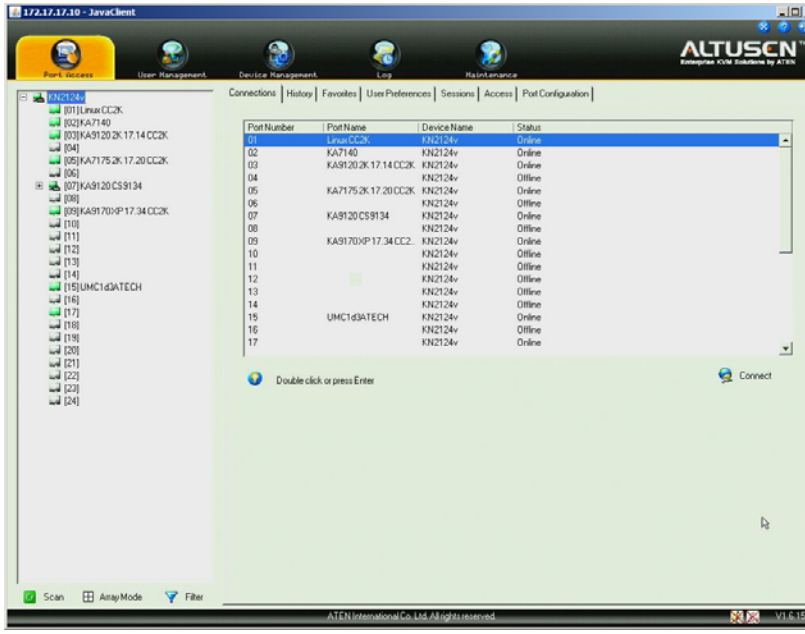
After the local console has been connected (see *Single Stage Installation*, page 25), and the KVM over IP switch turned on, a login prompt appears on the console monitor:



Since this is the first time you are logging in, use the default Username: *administrator*; and the default Password: *password*.

Note: For security purposes, you should change these to a unique Username and Password. (See *Changing the Super Administrator Login*, page 40 for details.)

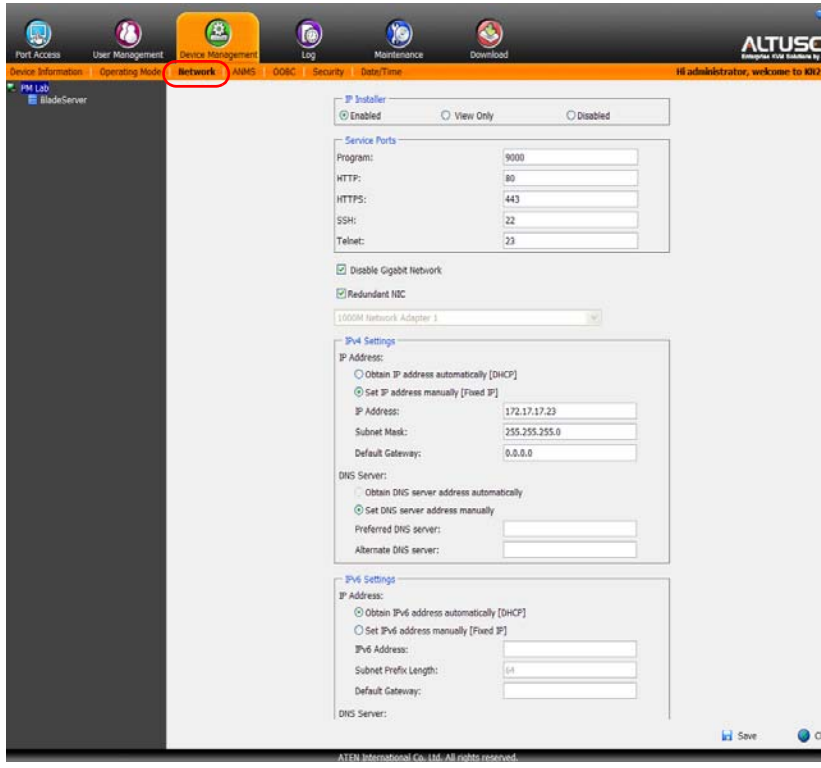
After you successfully log in, the Local Console Main Page appears:



Network Setup

To set up the network, do the following:

1. Click the **Device Management tab.**
2. Select the **Network** tab.



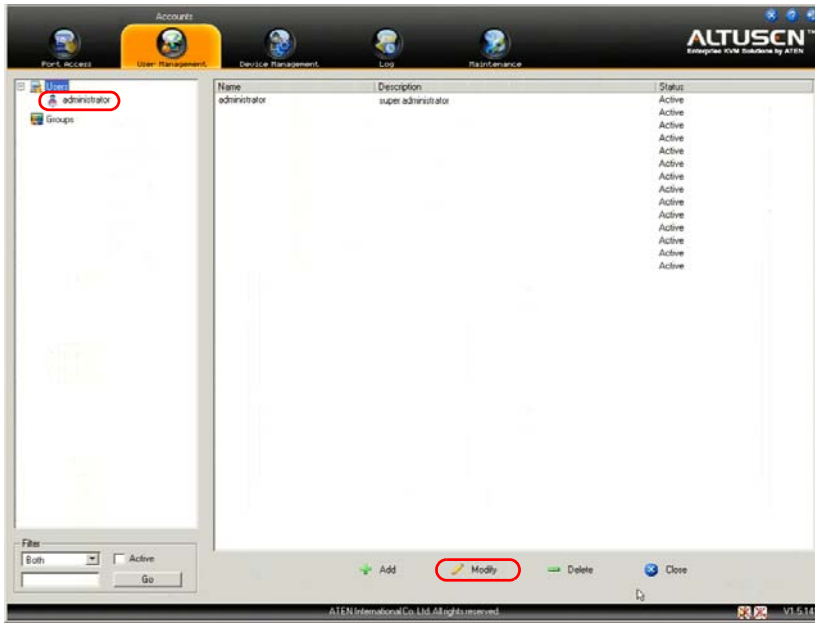
3. Fill in the fields according to the information provided under *Network*, page 157.

Changing the Super Administrator Login

To change the default Super Administrator Username and Password, do the following:

1. At the top of the screen, click the **User Management** tab.

   The User Management page has a list of Users and Groups in the Sidebar at the left, and a more detailed list of users – with more information about them – in the large central panel. Since this is the first time the page is being accessed, only the Super Administrator appears:

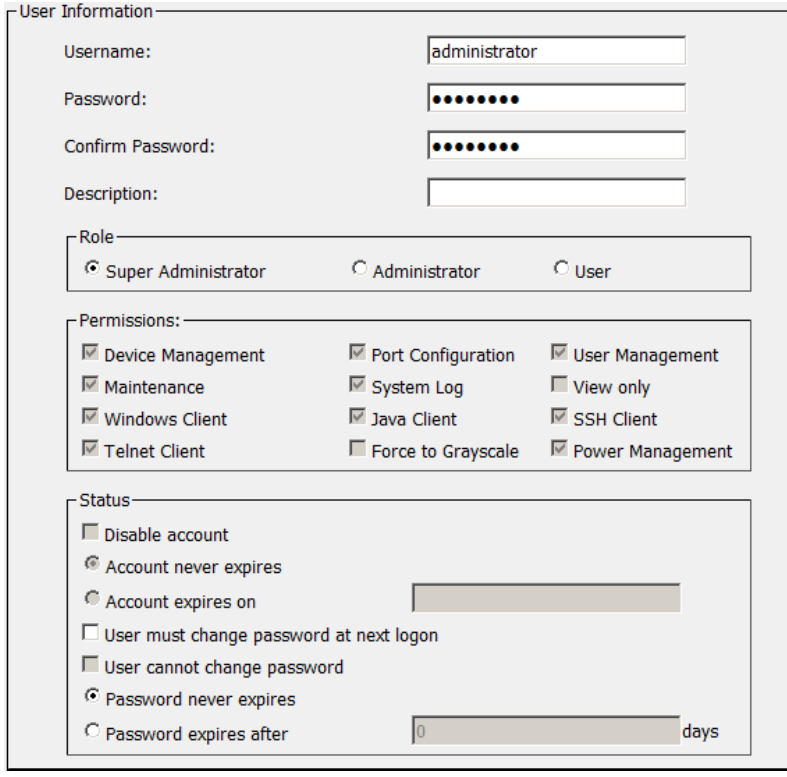


2. Click **administrator** in the left panel

   – or –

   Select *administrator* in the central panel, then click **Modify** (at the bottom of the page.)

The *User Information* page appears:



3. Change the Username and Password to something unique.
4. Enter the password again in the *Confirm Password* field to confirm it is correct.
5. Click **Save**.
6. When the dialog box informing you that the change completed successfully appears, Click **OK**.
7. Click on another item on the Local Console Main Page, to close this page.

Moving On

After setting up the network and changing the default Super Administrator password, you can proceed to other administration activities. These include User Management, Device Management, and Firmware Upgrade Maintenance.

These activities can be accomplished using any of the KVM over IP switch's GUI utilities. These include the Local Console; the browser-based Windows ActiveX Viewer; the browser-based Java Client Viewer; the stand-alone Windows Client AP; and the stand-alone Java Client AP. Choose the approach that suits you best.

Note: Firmware Upgrade Maintenance cannot be performed from the local console. You must log in remotely with one of the KVM over IP switch's other GUI utilities for this operation.

Chapter 4
Logging In

Overview

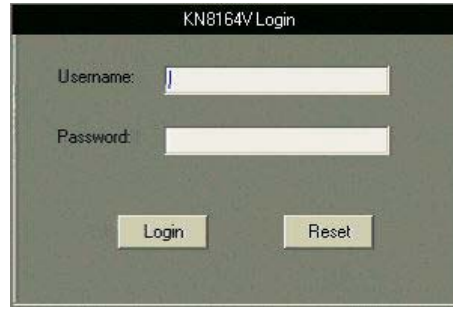
KVM over IP switches can be accessed from a local console; an Internet browser; a Windows application (AP) program; and a Java application (AP) program.

No matter which access method you choose, the KVM over IP switch's authentication procedure requires you to submit a valid username and password. If you supply invalid login information, the authentication routine will return an *Invalid Username or Password*, or *Login Failed* message. If you see this type of message, log in again with a correct username and password.

Note: If the number of invalid login attempts exceeds a specified amount, a time out period is invoked. You must wait until the time out period expires before you can attempt to log in again. See *Login Failures*, page 173 for further details.

Local Console Login

When the local console is attached (see *Single Stage Installation*, page 25) and there is no user logged in, the KVM over IP switch's login screen appears on the monitor:



Simply key in your valid Username and Password, then click **Login** to bring up the Local Console Main Page. The Local Console Main Page is similar to the Web Browser, WinClient and Java Client Main Pages. For a description of the Web Browser Main Page, see page 53.

Browser Login

KVM over IP switches can be accessed via an Internet browser running on any platform. To access the switch, do the following:

1. Open the browser and specify the IP address of the switch you want to access in the browser's location bar.

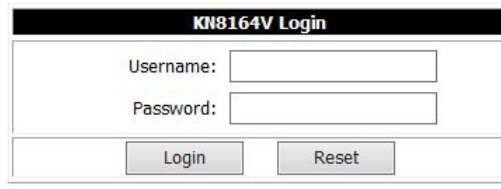
   Note: For security purposes, a login string may have been set by the administrator (see page 177 for details). If so, you must include a forward slash and the login string along with the IP address when you log in. For example:

   ```
   192.168.0.100/kn8164v
   ```

   If you don't know the IP address and login string, ask your Administrator.

2. When a Security *Alert* dialog box appears, accept the certificate – it can be trusted. (See *Trusted Certificates*, page 268, for details.) If a second certificate appears, accept it as well.

   Once you accept the certificate(s), the login page appears:

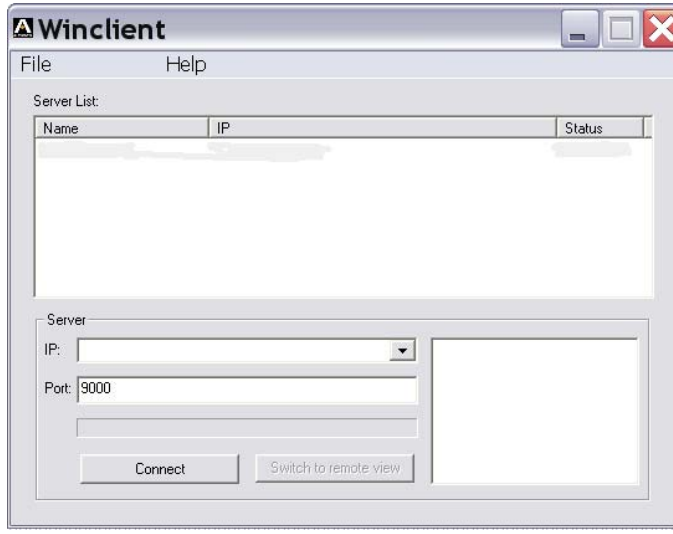


3. Provide your username and password (set by the administrator), then click **Login** to bring up the Web Main Page. For a discussion of the Web Main Page, see page 53.

Windows Client AP Login

In some cases, the Administrator may not want the KVM over IP switch to be available via browser access. The Windows AP Client allows direct remote access to Windows systems users, without having to go through a browser (although you initially download the Windows AP Client program from the browser page – see Chapter 11, *Download*).

To connect to the KVM over IP switch, go to the location on your hard disk that you downloaded the Windows AP Client program to, and double-click its icon (*WinClient.exe*) to bring up the Windows Client Connection Screen:



The Windows Client AP Connection Screen

A description of the Connection Screen is given in the following table:

Item	Description
Menu Bar	The Menu Bar contains two items: File and Help. ◆ The *File Menu* allows the operator to Create, Save, and Open user created Work files (see *The File Menu*, page 48). ◆ The *Help Menu* displays the WinClient AP version.
Server List	Each time the WinClient.exe file is run, it searches the user's local LAN segment for KVM over IP switches, and lists whichever ones it finds in this box. If you want to connect to one of these units, **double-click** it. (See *Connecting – Windows Client AP*, page 47 for details.) **Note:** 1. The switch will not appear in the list unless its *Enable Device List* configuration parameter has been enabled. See *Operating Mode*, page 155 for details. 2. Only units whose Access Port settings for *Program* (see *Service Ports*, page 158) match the number specified for *Port* in the Server area of this dialog box appear in the Server List window.
Server	This area is used when you want to connect to a KVM over IP switch at a remote location. You can drop down the IP list box and select an address from the list. If the address you want isn't listed, you can key in the target IP address in the IP field, and its port number in the Port field. (If you don't know the port number, contact your Administrator.) ◆ When the IP address and Port number have been specified, click **Connect**. (See *Connecting – Windows Client AP*, page 47 for details.) ◆ When you have finished with your session and come back to this dialog box, click **Disconnect** to end the connection.
Message Panel	Located just to the right of the Server panel, the Message panel lists status messages regarding the connection to the KVM over IP switch.
Switch to Remote View	Once you have been authenticated (see *Connecting – Windows Client AP*, page 47 for details), this button becomes active. Click it to switch to the GUI Main Page. The GUI Main Page is described on page 56.

Connecting – Windows Client AP

To connect to a KVM over IP switch do the following::

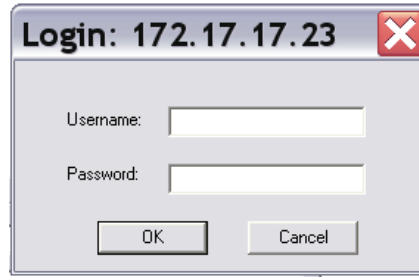
1. From the *Server List* box, **double-click** the device that you wish to connect to.

   – Or –

   Specify its IP address and port number in the *Server IP* and *Port* input boxes.

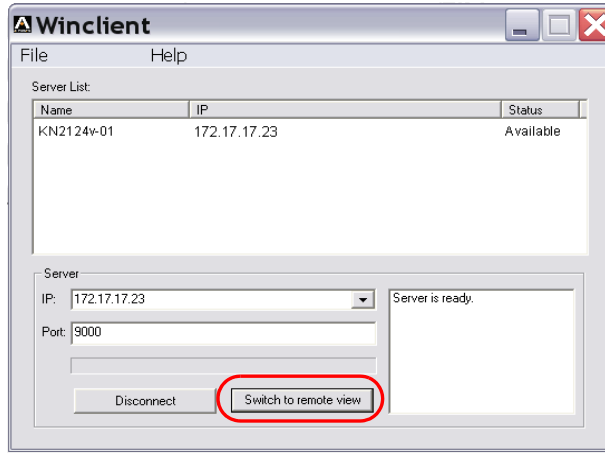
2. Click **Connect**.

   The *Login* dialog box appears:



3. Key in a valid Username and Password, and then click **OK**.

4. Once you have been authenticated, the *Switch to Remote View* button becomes active. Click it to connect to the switch and bring up its GUI Main Page. For a description of the GUI Main Page, see page 48.



The File Menu

The *File Menu* allows the operator to Create, Save, and Open user created Work files. A Work File consists of all the information specified in a Client session. This includes the Server List and Server IP list items, as well as the Hotkey settings.

Whenever a user runs the Client program, it opens with the values contained in the *current work file*. The current work file consists of the values that were in effect the last time the program was closed.

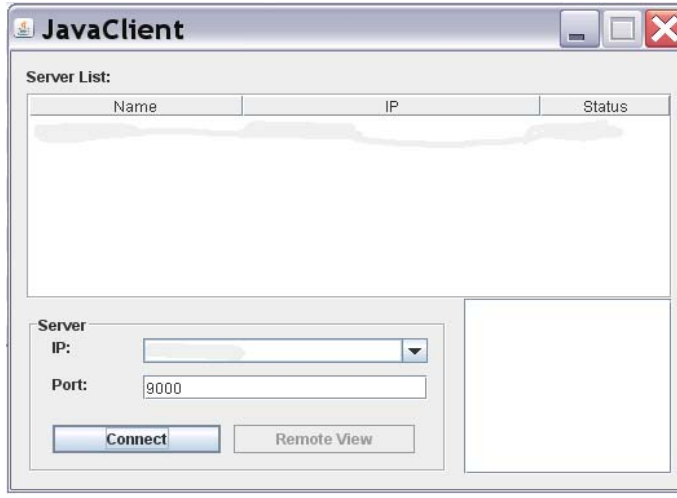
The File menu consists of the following items:

New	Allows the user to create a named work file so its values will not be lost, and it will be available for future recall.
Open	Allows the user to open a previously saved work file and use the values contained in it.
Save	Allows the user to save the values presently in effect as the *current work file*.
Exit	Exits the WinClient.

Java Client AP Login

In those cases in which the Administrator does not want the KVM over IP switch to be available via browser access, but the local client users aren't running Windows, the Java AP Client provides direct remote access to non-Windows systems users (although you initially download the Java AP Client program from the browser page – see Chapter 11, *Download*).

To connect to the KVM over IP switch, go to the location on your hard disk that you downloaded the Java AP Client program to, and double-click its icon (*JavaClient.jar*) to bring up the Java Client Connection Screen:



The Java Client AP Connection Screen

A description of the Connection Screen is given in the following table:

Item	Description
Server List	Each time the JavaClient.jar file is run, it searches the User's local LAN segment for KVM over IP switches, and lists whichever ones it finds in this box. If you want to connect to one of these units, **double-click** it. (See *Connecting – Windows Client AP*, page 47 for details.) **Note:** 1. The switch will not appear in the list unless its *Enable Device List* configuration parameter has been enabled. See *Operating Mode*, page 155 for details. 2. Only units whose Access Port settings for *Program* (see *Service Ports*, page 158) match the number specified for *Port* in the Server area of this dialog box appear in the Server List window.
Server	This area is used when you want to connect to a KVM over IP switch at a remote location. You can drop down the IP list box and select an address from the list. If the address you want isn't listed, you can key in the target IP address in the IP field, and its port number in the Port field. (If you don't know the port number, contact your Administrator.) ◆ When the IP address and Port number have been specified, click **Connect**. (See *Connecting – Windows Client AP*, page 47 for details.) ◆ When you have finished with your session and come back to this dialog box, click **Disconnect** to end the connection.
Message Panel	Located just to the right of the Server panel, the Message panel lists status messages regarding the connection to the KVM over IP switch.
Switch to Remote View	Once you have been authenticated (see *Connecting – Windows Client AP*, page 47 for details), this button becomes active. Click it to switch to the GUI Main Page. The GUI Main Page is described on page 56.

Connecting – Java Client AP

To connect to a KVM over IP switch do the following::

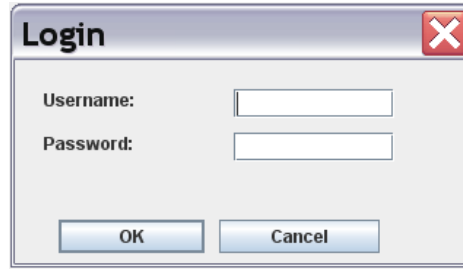
1. From the *Server List* box, **double-click** the device that you wish to connect to.

   – Or –

   Specify its IP address and port number in the *Server IP* and *Port* input boxes.

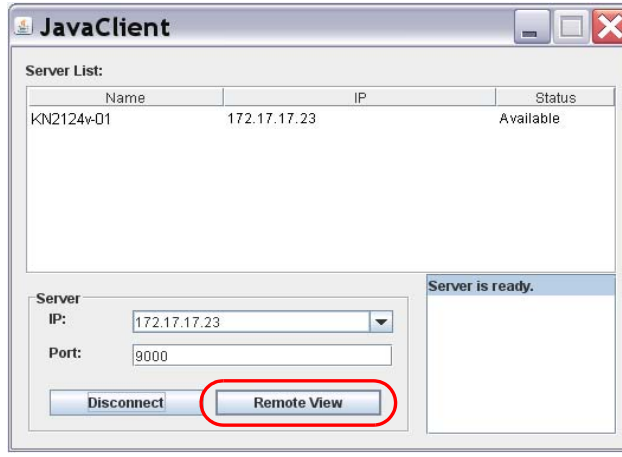
2. Click **Login**

   The *Login* dialog box appears:



3. Key in a valid Username and Password, and then click **OK**.

4. Once you have been authenticated, the *Remote View* button becomes active. Click it to connect to the switch and bring up its GUI Main Page. For a description of the GUI Main Page, see page 48.



This Page Intentionally Left Blank

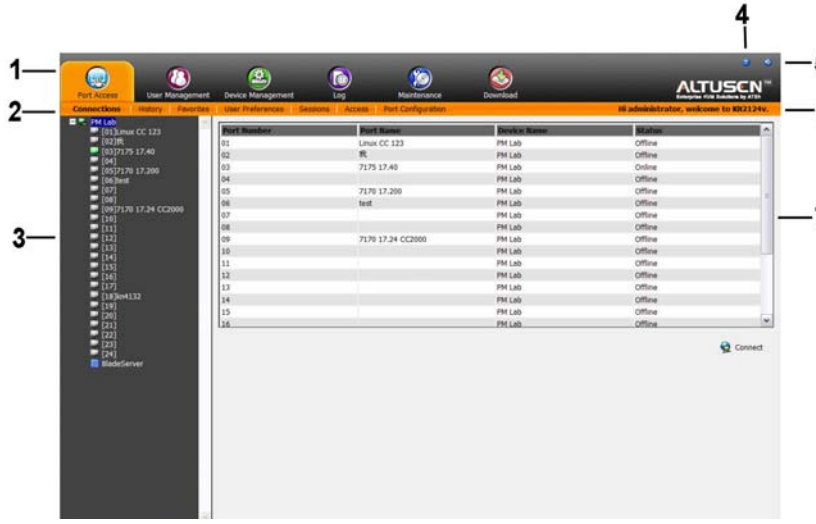
Chapter 5
The User Interface

Overview

Once you have successfully logged in, the KVM over IP switch's user interface Main Page appears. The look of the page varies slightly, depending on which method you used to log in. Each of the interfaces is described in the sections that follow.

The Web Browser Main Page

To ensure multi-platform interoperability, access to the KVM over IP switches can be accomplished with most standard web browsers. Once users log in and are authenticated (see page 44), the *Web Browser Main Page* comes up, with the Port Access page displayed:



Note: The screen depicts a Super Administrator's page. Depending on a user's type and permissions, not all of these elements appear.

Page Components

The web page screen components are described in the table, below:

No.	Item	Description
1	Tab Bar	The tab bar contains the KVM over IP switch's main operation categories. The items that appear in the tab bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
2	Menu Bar	The menu bar contains operational sub-categories that pertain to the item selected in the tab bar. The items that appear in the menu bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
3	Sidebar	The Sidebar provides a tree view listing of ports that relate to the various tab bar and menu bar selections. Clicking a node in the Sidebar brings up a page with the details that are relevant to it. There is a *Filter* button at the bottom of the Sidebar that lets you expand or narrow the scope of the ports that appear in the tree. The Filter function is discussed in detail on page 97
4	About	About provides information regarding the switch's current firmware version.
5	Logout	Click this button to log out of your KVM over IP switch session.
6	Welcome Message	If this function is enabled (see *Welcome Message**, page 118), a welcome message displays here.
7	Interactive Display Panel	This is your main work area. The screens that appear reflect your menu choices and Sidebar node selection.

The Tab Bar

The number and type of icons that appear on the Tab Bar at the top of the page are determined by the user's type (Super Administrator, Administrator, User) and the permissions assigned when the user's account was created. The functions associated with each of the icons are explained in the table below:

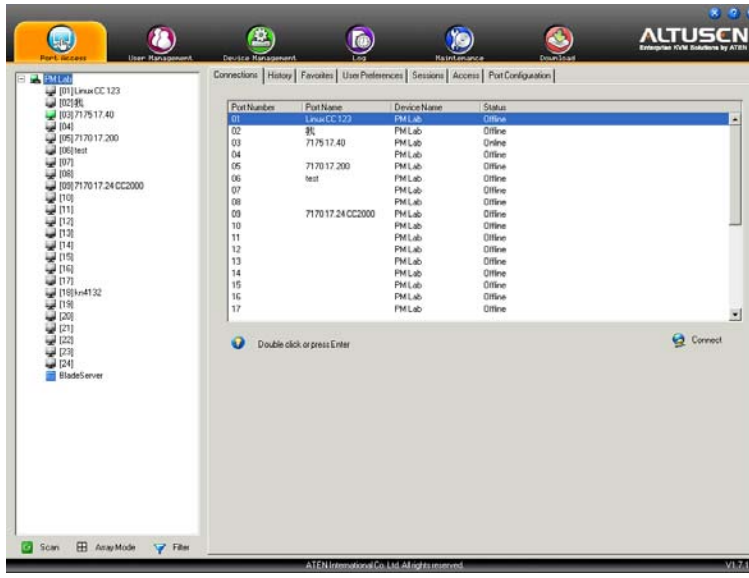
Icon	Function
	Port Access: The Port Access page is used to access and control the devices on the KVM over IP switch installation. This page is available to all users.
	User Management: The User Management page is used to create and manage Users and Groups. It can also be used to assign devices to them. User Management is discussed on page 135. This tab is available to the Super Administrator, as well as administrators and users who have been given User Management permission. The tab doesn't appear for other administrators and users.
	Device Management: The Device Management page is used to configure and control the overall operation of the KVM over IP switch. This page is available to the Super Administrator, as well as administrators and users who have been given Device Management permission. The tab doesn't appear for other administrators and users.
	Log: The Log page displays the contents of the log file. The Log page is discussed on page 191.
	Maintenance: The Maintenance page is used to install new firmware; backup and restore configuration and account information; ping network devices; and restore default values. The Maintenance page is discussed on page 195. This page is available to the Super Administrator (and Administrators and Users with *Maintenance* permission). The icon doesn't display on the page of ordinary administrators and users.
	Download: Users can click this icon to download AP versions of the Windows Client; the Java Client; and the Log Server. This page is available to all users. The programs that can be downloaded depend on the user's permissions.

There are two small icons at the extreme right of the page. Their functions are described in the table, below:

Icon	Function
	Click this icon to brings up a panel with information about the KVM over IP switch firmware version.
	Click this icon to log out and end your KVM over IP switch session.

The AP GUI Main Page

With WinClient AP, and Java Client AP access, once users log in (see *Logging In*, page 43), the *GUI Main Page* comes up:



The GUI Main Page is similar to that of the Web Browser. The differences between them are as follows:

1. The AP GUI version doesn't have a menu bar below the tab bar; it has a series of tabs like a notebook, instead. Like the Web Browser interface, however, the makeup of the tabbed notebook changes depending on the items selected on the main Tab Bar and in the Sidebar.
2. In addition to *Filter*, there are also buttons for *Scan* and *Array Mode* at the bottom of the Sidebar. These functions are discussed in Chapter 6, *Port Access*.
3. There is a hidden *Control Panel* at the upper or lower center of the screen that becomes visible when you mouse over it. (The default is at the upper center of the screen.)

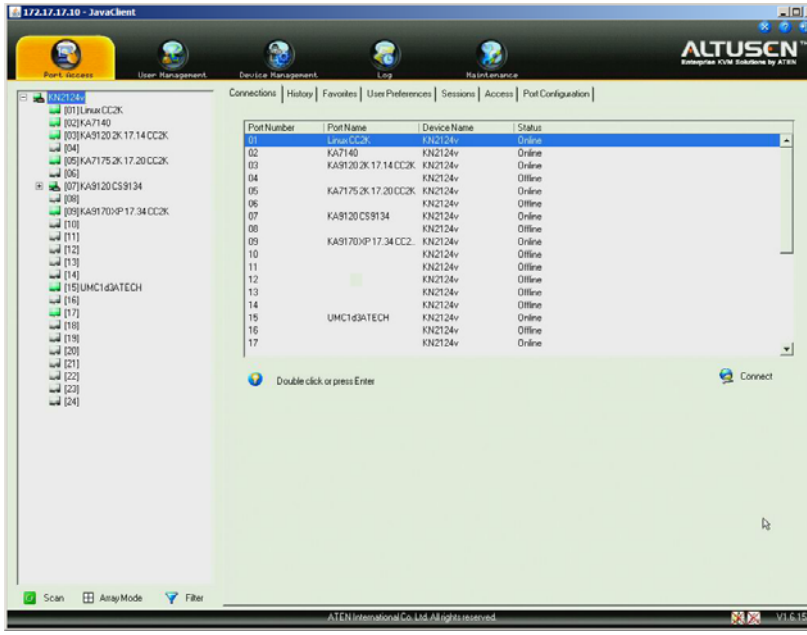
4. There is an additional icon at the extreme right of the page: . Click this icon to close the GUI Main Page and go to the display of the last selected port.

5. The GUI can be navigated via the keyboard as shown in the table, below:

Keys	Action
Ctrl + P	Opens the Port Access page.
Ctrl + U	Opens the User Management page.
Ctrl + D	Opens the Device Management page.
Ctrl + L	Opens the Log page.
Ctrl + M	Opens the Maintenance page.
Ctrl + A	Opens the Download page.
F1	To see *About* information
F2	To edit the port name of the selected port.
F4	Selects the Sidebar (left) panel.
F5	Selects the main (right) panel
F7	Closes the GUI.
F8	To log out.

The Local Console GUI Main Page

The Local Console GUI Main Page is similar to the Java and Windows AP GUI Main Page:



The major difference is that the Local Console Main Page doesn't have a tab for *Download*.

In addition, there are two small icons at the bottom right – as described in the following table.

Icon	Function
	Speaker. Allows sound output from the servers connected to the switch's ports to be heard on the speakers connected to the Local Console. Click the icon to toggle speaker support On and Off. When Off, a red **X** displays across the icon.
	Microphone. Allows microphone input from the Local Console to be sent to the servers connected to the switch's ports. Click the icon to toggle microphone support On and Off. When Off, a red **X** displays across the icon.

The Control Panel

WinClient Control Panel

Since the WinClient Control Panel (for the ActiveX Web Viewer and WinClient AP) contains the most complete functionality, this section describes the WinClient Control Panel. Although the Java Control Panel (for the Web Viewer and Java Client AP) does not enable all of the features that this one does, the functions that they do share are the same, and you can refer to the information described here when using it.

The Control Panel is hidden at the upper or lower center of the screen (the default is at the upper center), and becomes visible when you mouse over it. The panel consists of three rows: an icon row at the top, and two text rows below it:

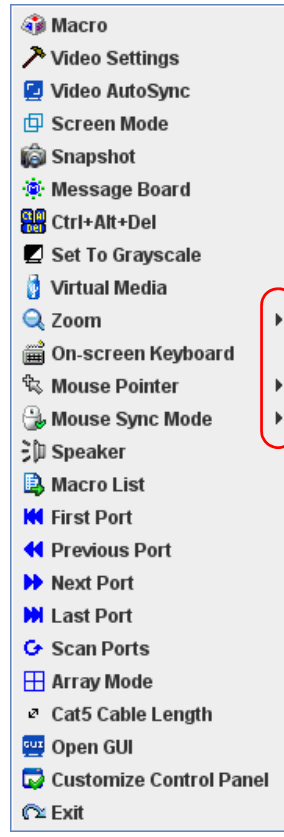
Note: The above image shows the complete Control Panel. The icons that appear can be user selected. See *Control Panel Configuration*, page 90, for details.

- By default, the upper text row shows the video resolution of the remote display. As the mouse pointer moves over the icons in the icon bar, however, the information in the upper text row changes to describe the icon's function. In addition, if a message from another user is entered in the message board, and you have not opened the message board in your session, the message will appear in the upper row.
- The lower row shows the IP address of the device you are accessing at the left of the row. The center of the row indicates which bus the user is on (the number before the slash), and the total number of users on that bus (the number behind the slash).

Note: 1. The bus and user information in the center of the row only displays if it has been enabled. See *Bus Info*, page 91 for details.

2. See *Multiuser Operation*, page 218 for further information regarding the KVM over IP switch's bus assignments.

- Right clicking in the text row area brings up a menu-style version of the toolbar. In addition, it allows you to select options for the *Zoom*, *Mouse Pointer*, and *Mouse Sync Mode*. These functions are discussed in the sections that follow.



- To move the Control Panel to a different location on the screen, place the mouse pointer over the text row area, then click and drag.

WinClient Control Panel Functions

The Control Panel functions are described in the table below.

Icon	Function
	This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.
	Click to bring up the Macros dialog box (see page 64 for details).
	Click to bring up the Video Options dialog box. Right-click to perform a quick Auto Sync (see *Video Settings*, page 73, for details).
	Click to perform a video and mouse autosync operation. It is the same as clicking the Auto-sync button in the *Video Options* dialog box (see *Video Settings*, page 73).
	Toggles the display between *Full Screen Mode* and *Windowed Mode*.
	Click to take a snapshot (screen capture) of the remote display. See *Snapshot*, page 91, for details on configuring the Snapshot parameters.
	Click to bring up the Message Board (see *The Message Board*, page 78).
	Click to send a Ctrl+Alt+Del signal to the remote system.
	Click to toggle the remote display between color and gray scale views.
	Click to bring up the *Virtual Media* dialog box. The icon changes depending on the status of the virtual media function. See *Virtual Media*, page 80, for specific details. Note: This icon displays in gray when the function is disabled or not available.
	Click to zoom the remote display window. **Note:** This feature is only available in windowed mode (Full Screen Mode is off). See *Zoom*, page 83 for details.
	Click to bring up the on-screen keyboard (see *The On-Screen Keyboard*, page 84).
	Click to select the mouse pointer type. **Note:** This icon changes depending on which mouse pointer type is selected (see *Mouse Pointer Type*, page 86).

	Click to toggle Automatic or Manual mouse sync. ◆ When the selection is *Automatic*, a green √ appears on the icon. ◆ When the selection is *Manual*, a red X appears on the icon. See *Mouse DynaSync Mode*, page 88 for a complete explanation of this feature.
	Click to toggle sound from the remote server to be heard on the client computer's speakers on or off. The "prohibited" symbol (a red circle with a diagonal bar) displays on the icon when the speaker is toggled Off.
	Click to display a dropdown list of *User* macros in order to access and run macros more conveniently than using the Macros dialog box (see the *Macros* icon in the table above, and the *Macros* section on page 64).
	The Power Over the Net™ icon allows the device to be powered on, powered off or rebooted, when the device is connected to a compatible PON "PN" series unit. (For more information on configuring PON features see *PON Devices*, page 186). See *Power Over the Net*™, page 87 for a complete explanation of this feature.
	Under an accessed port, click to skip to the first port accessible to the user on the entire installation without having to recall the Port Access page.
	Under an accessed port, click to skip to the first port accessible to the user that is previous to the current one without having to recall the Port Access page.
	Under an accessed port, click to skip to the first port accessible to the user that is after the current one without having to recall the Port Access page.
	Under an accessed port, click to skip to the last port accessible to the user on the entire installation without having to recall the Port Access page.
	Under an accessed port, click to begin Auto Scan Mode. The KVM over IP switch automatically switches among the ports that were selected for Auto Scanning with the *Filter* function (see *Filter*, page 97). This allows you to monitor their activity without having to switch among them manually.
	Under an accessed port, click to invoke Panel Array Mode (see *Panel Array Mode*, page 216).
	Under an accessed port, click to recall the GUI.
	Click to bring up the Control Panel Configuration dialog box. See *Control Panel Configuration*, page 90, for details on configuring the Control Panel.

	Click to exit the viewer. ◆ Exiting from a Browser Viewer session brings you back to the web browser Main Page. ◆ Exiting from a WinClient AP session brings you back to the login dialog box (see page 45). ◆ Exiting from a Java Client AP session brings you back to the login dialog box (see page 49).
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. ◆ When the lock state is *On*, the LED is bright green and the lock hasp is closed. ◆ When the lock state is *Off*, the LED is dull green and the lock hasp is open. Click on the icon to toggle the status. **Note:** These icons and your local keyboard icons are in sync. Clicking an icon causes the corresponding LED on your keyboard to change accordingly. Likewise, pressing a Lock key on your keyboard causes the icon's color to change accordingly.

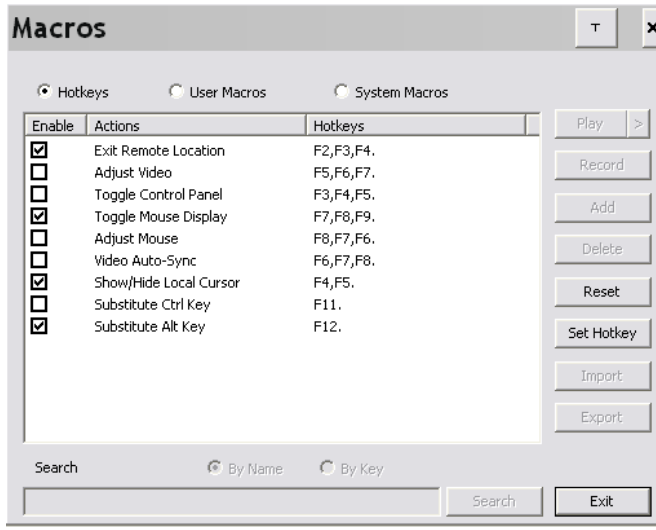
Macros

The Macros icon provides access to three functions found in the Macros dialog box: Hotkeys, User Macros, and System Macros. Each of these functions is described in the following sections.

Hotkeys

Various actions related to manipulating the remote server can be accomplished with hotkeys. The *Hotkey Setup* utility (accessed by clicking this icon), lets you configure which hotkeys perform the actions.

The hotkeys that invoke an action are shown to the right of its name. Use the checkbox to the left of an action's name to enable or disable its hotkey.



To change the hotkey for an action, do the following:

1. Highlight the *Action*, then click **Set Hotkey**.
2. Press your selected Function keys (one at a time). The key names appear in the *Hotkeys* field as you press them.
   - You can use the same function keys for more than one action, as long as the key sequence is not the same.
   - To cancel setting a hotkey value, click **Cancel**; to clear an action's Hotkeys field, click **Clear**.
3. When you have finished keying in your sequence, click **Save**.

To reset all the hotkeys to their default values, click **Reset**.

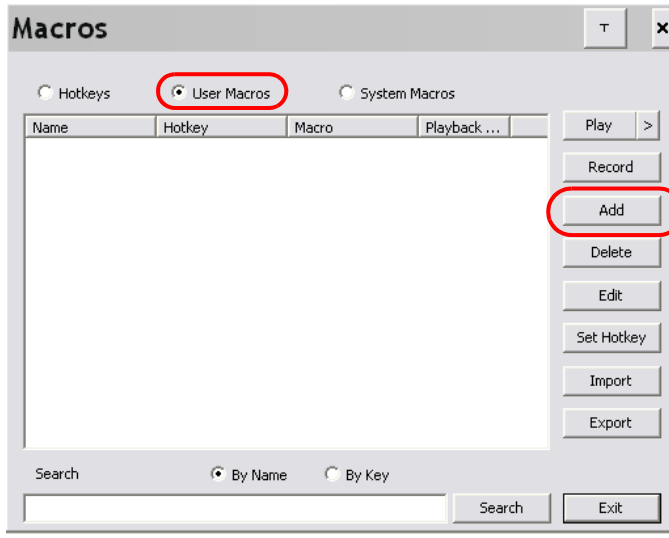
An explanation of the Hotkey actions is given in the table below:

Action	Explanation
Exit remote location	Breaks the connection to the KVM over IP switch and returns you to local client computer operation. This is equivalent to clicking the *Exit* icon on the Control Panel. The default keys are F2, F3, F4.
Adjust Video	Brings up the *Video Settings* dialog box. This is equivalent to clicking the *Video Settings* icon on the Control Panel. The default keys are F5, F6, F7.
Toggle Control Panel	Toggles the Control Panel Off and On. The default keys are F3, F4, F5.
Toggle mouse display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to shrink the non-functioning pointer down to a barely noticeable tiny circle, which can be ignored. Since this function is a toggle, use the hotkeys again to bring the mouse display back to its original configuration. This is equivalent to selecting the *Dot* pointer type from the *Mouse Pointer* icon on the Control Panel. The default keys are F7, F8, F9. **Note:** The Java Control Panel does not have this feature.
Adjust mouse	This synchronizes the local and remote mouse movements. The default keys are F8,F7,F6.
Video Auto-sync	This combination performs an auto-sync operation. It is equivalent to clicking the *Video Autosync* icon on the Control Panel. The default keys are F6,F7,F8.
Show/Hide Local Cursor	Toggles off and on: hides local cursor and locks the mouse pointer and keyboard use within the Windows/Java Client AP window, plus hides the control panel. This is equivalent to selecting the *Single* pointer type from the *Mouse Pointer* icon on the Control Panel. The default keys are F4,F5.
Substitute Ctrl key	If your local client computer captures Ctrl key combinations, preventing them from being sent to the remote server, you can implement their effects on the remote server by specifying a function key to substitute for the Ctrl key. If you substitute the F11 key, for example, pressing [F11 + 5] would appear to the remote server as [Ctrl + 5]. The default key is F11.
Substitute Alt key	Although all other keyboard input is captured and sent to the KVM over IP switch, [Alt + Tab] and [Ctrl + Alt + Del] work on your local client computer. In order to implement their effects on the remote server, another key may be substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del]. The default key is F12.

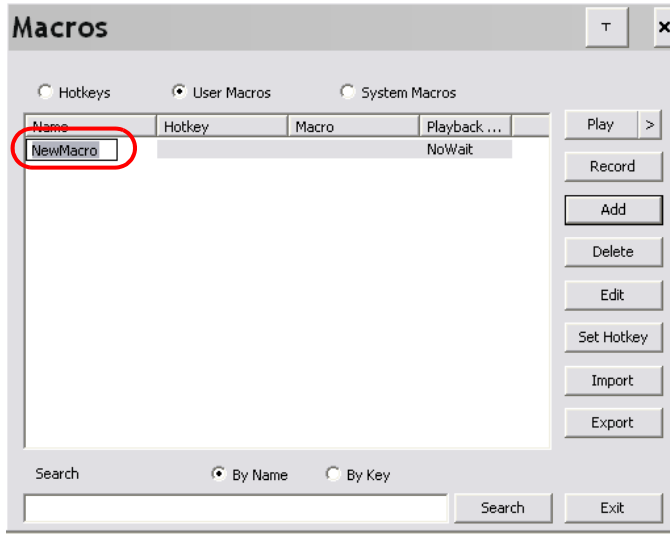
User Macros

User Macros are created to perform specific actions on the remote server. To create the macro, do the following:

1. Select *User Macros*, then click **Add**.



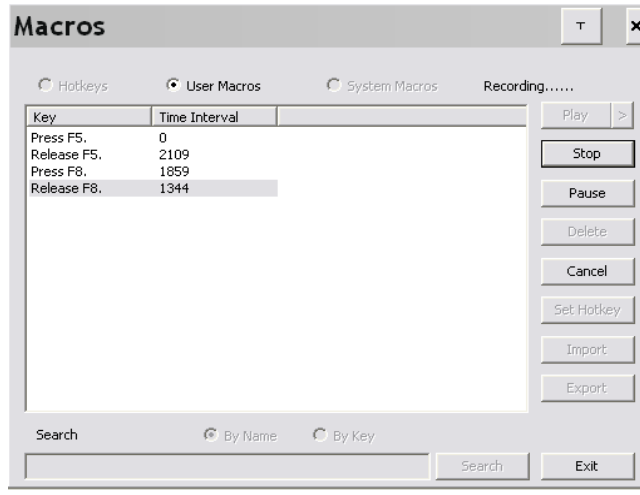
2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:



3. Click **Record**.

   The dialog box disappears, and a small panel appears at the top left of the screen:

4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Pause** again.
   - Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes:



   - Clicking **Cancel** cancels all keystrokes.
   - When you have finished, click **Stop**. (This is the equivalent of clicking *Done* in Step 5.)

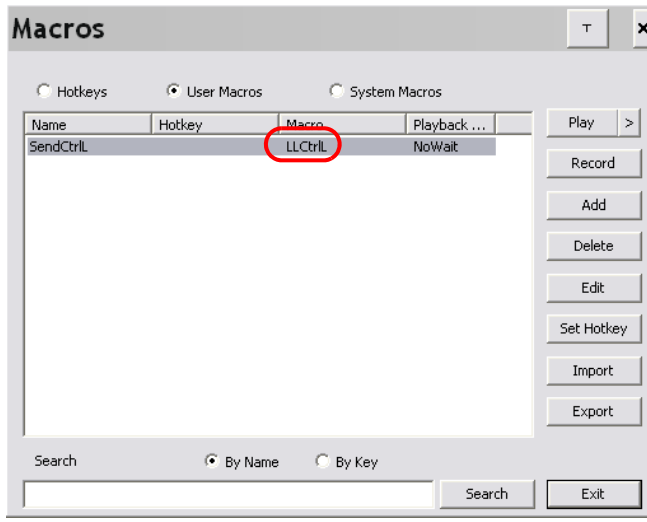
Note: 1. Case is not considered – typing **A** or **a** has the same effect.

5. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.

2. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is **A** the alternate Chinese character obtained via keyboard switching is not recorded.

---

6. If you haven't brought up the Show dialog, click **Done** when you have finished recording your macro. You return to the Macros dialog box with your system macro key presses displayed in the Macro column:



7. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.

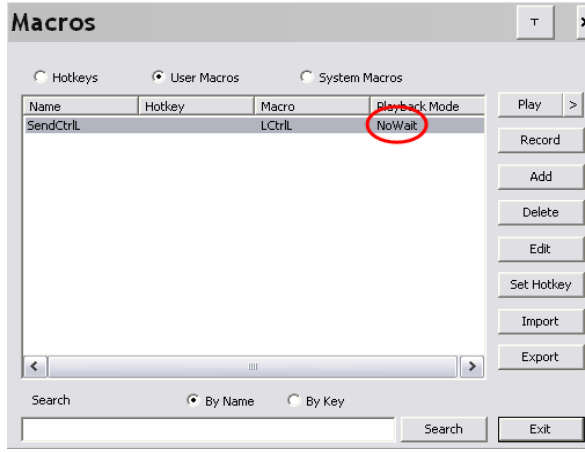
8. Repeat the procedure for any other macros you wish to create.

After creating your macros, you can run them in any of three ways:

1. By using the hotkey (if one was assigned).
2. By opening the Macro List on the Control Panel and clicking the one you want (see page 62).
3. By opening this (Macros) dialog box and clicking **Play**.

If you run the macro from this dialog box, you have the option of specifying how the macro runs.

- If you choose *Play Without Wait*, the macro runs the key presses one after another with no time delay between them.
- If you choose *Play With Time Control*, the macro waits for the amount of time between key presses that you took when you created it. Click on the arrow next to *Play* to make your choice.
- If you click *Play* without opening the list, the macro runs with the default choice (*NoWait* or *TimeCtrl*), which is shown in the *Playback* column.



You can change the default choice by clicking on the current choice (*NoWait* in the screenshot above), and selecting the alternate choice.

Note: 1. Information about the Search function is given on page 70.

2. User Macros are stored on the Local Client computer of each user. Therefore, there is no limitation on the of number of macros, the size of the macro names, or makeup of the hotkey combinations that invoke them

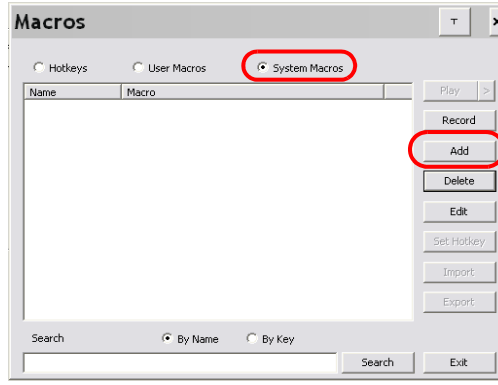
■ Search

Search, at the bottom of the dialog box, lets you filter the list of macros that appear in the large upper panel for you to play or edit. Click a radio button to choose whether you want to search by name or by key; key in a string for the search; then click **Search**. All instances that match your search string appear in the upper panel.

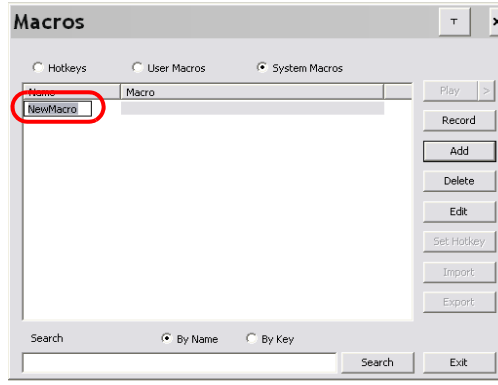
System Macros

System Macros are used to create exit macros for when you close a session. For example, as an added measure of security, you could create a macro that sends the Winkey-L combination which would cause the remote server's log in page to come up the next time the device was accessed. To create the macro, do the following:

1. Select *System Macros*, then click **Add**.



2. In the dialog box that comes up, replace the "New Macro" text with a name of your choice for the macro:



3. Click **Record**.

   The dialog box disappears, and a small panel appears at the top left of the screen:

4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Pause** again.
   - Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes (see page 71).

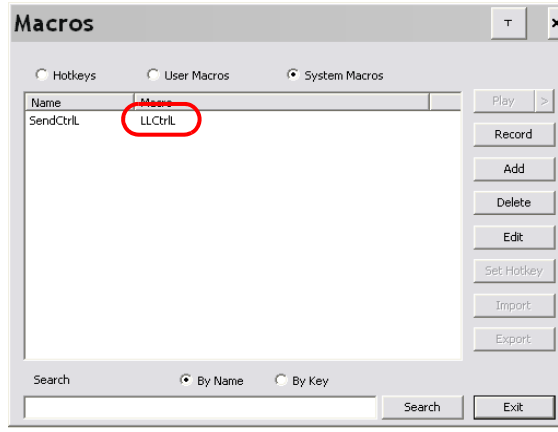
Note: 1. Case is not considered – typing **A** or **a** has the same effect.

5. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.

2. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is **A** the alternate Chinese character obtained via keyboard switching is not recorded.

---

6. If you haven't brought up the Show dialog, click **Done** when you have finished recording your macro. You return to the Macros dialog box with your system macro key presses displayed in the Macro column:



7. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.

8. Repeat the procedure for any other macros you wish to create.

Once the system macros have been created, they are available for use on a port-by-port basis. They get selected on a port's *Port Configuration* → *Port Properties* page (see *Port Level*, page 127 for details).

Note: 1. Information about the Search function is given on page 70.

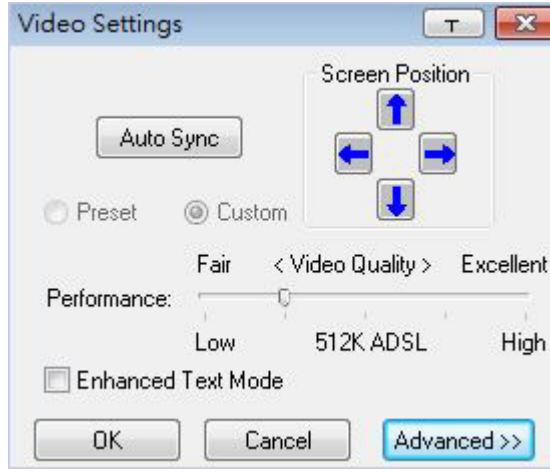
2. You can choose only one system macro per port.

3. Systems macros are stored on the switch, therefore macro names may not exceed 64 Bytes; hotkey combinations may not exceed 256 Bytes. (Each key usually takes 3–5 Bytes.)

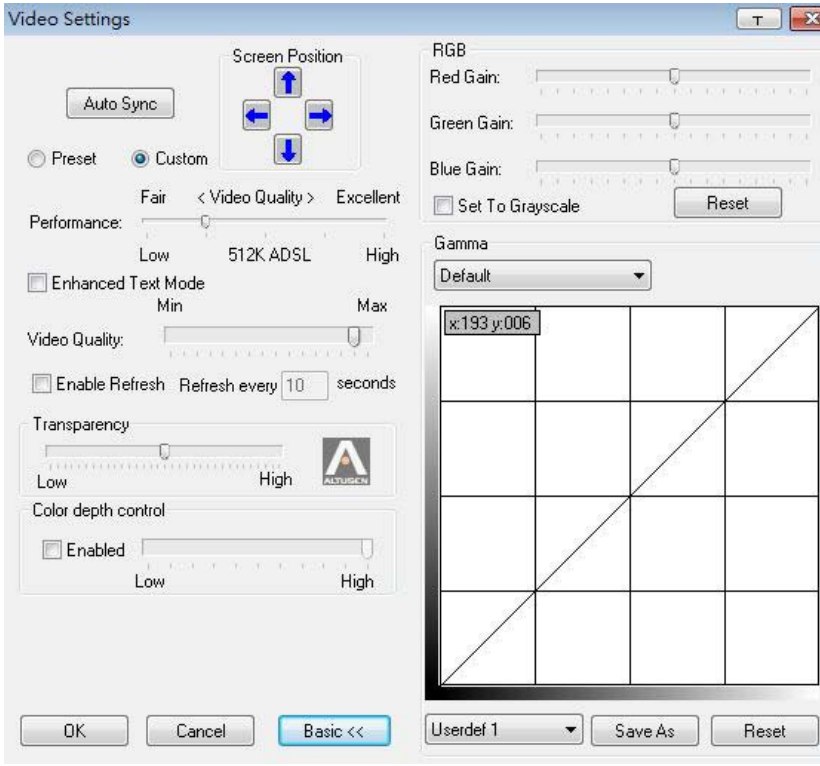
Video Settings

Clicking the *Hammer* icon on the Control Panel brings up the *Basic Video Settings* dialog box with basic settings. The options in the basic dialog box allow you to adjust the Screen Position, set Auto-Sync, and slide the Performance bar setting. Selecting the *Advanced* button opens the *Advanced Video Settings* dialog box, providing more detailed options including; RGB, Gamma, Video Quality, Enable Refresh, Transparency and Color Depth Control, as shown below:

Basic Video Settings



Advanced Video Settings



The meanings of the video adjustment options are given in the table:

Options	Usage
Screen Position	Adjust the horizontal and vertical position of the remote server window by Clicking the Arrow buttons.
Auto-Sync	Click Auto-Sync to have the vertical and horizontal offset values of the remote screen detected and automatically synchronized with the local screen. **Note:** 1. If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync. 2. This function works best with a bright screen. 3. If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually.

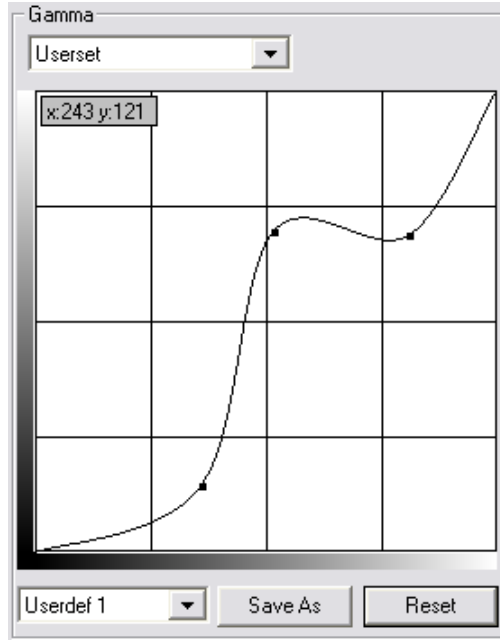
Options	Usage
RGB	Drag the slider bars to adjust the RGB (Red, Green, Blue) values. When a RGB value is increased, the RGB component of the image is correspondingly increased. If you enable *Set to Grayscale*, the remote video display is changed to grayscale. Clicking the *Reset* button brings the RGB settings back their default values.
Gamma	This section allows you to adjust the video display's gamma level. This function is discussed in detail in the next section, *Gamma Adjustment*.
Performance	Use the slide bar to select the type of Internet connection that the local client computer uses. The switch will use that selection to automatically adjust the *Video Quality* settings to optimize the quality of the video display. Since network conditions vary, if none of the pre-set choices seem to work well, you can select *Advanced* and use the Video Quality slider bar to adjust the settings to suit your conditions.
Enhanced Text Mode	Check this to solve video display problems related to video screen resolution that affect some interface systems (e.g., Sun Blade 1000 and other servers). This setting can improve the image color on some displays. Default YUV: 4:1:1 Enhanced Text Mode YUV: 4:4:4
Video Quality	Drag the slider bar to adjust the overall Video Quality. The larger the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may adversely effect response time.
Enable Refresh	The KVM over IP switch can redraw the screen every 1 to 99 seconds, eliminating unwanted artifacts from the screen. Select **Enable Refresh** and enter a number from 1 through 99. The KVM over IP switch will redraw the screen at the interval you specify. This feature is disabled by default. Click to put a check mark in the box next to *Enable Refresh* to enable this feature. **Note:** 1. The switch starts counting the time interval when mouse movement stops. 2. Enabling this feature increases the volume of video data transmitted over the network. The lower the number specified, the more often the video data is transmitted. Setting too low a value may adversely affect overall operating responsiveness.
Transparency	Adjusts the transparency of the toolbar that comes up when the GUI hotkey ([Scroll Lock][Scroll Lock], for example), is invoked. Slide the bar until the display in the example window is to your liking.

Options	Usage
Color Depth Control	This setting determines the richness of the video display by adjusting the amount of color information.
Preset / Custom	Using the Preset and Custom buttons allow you to set and save custom video settings, and revert back to default video settings.

Gamma Adjustment

If it is necessary to correct the gamma level for the remote video display, use the *Gamma* function of the Video Settings dialog box.

- Under *Advanced* configuration, there are ten preset and four user-defined levels to choose from. Drop down the list box and choose the most suitable one.
- For greater control, clicking the *Advanced* button brings up the following dialog box:

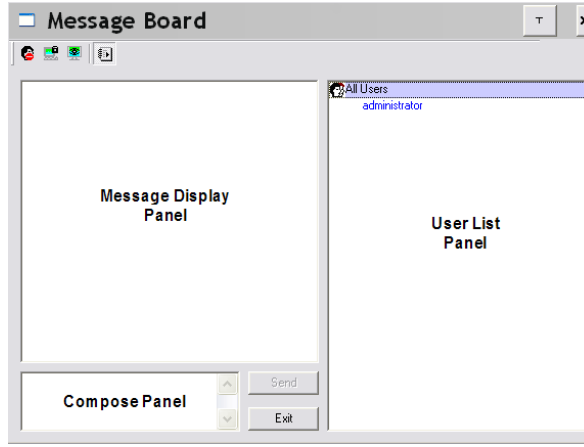


- Click and drag the diagonal line at as many points as you wish to achieve the display output you desire.
- Click **Save As** to save up to four user-defined configurations derived from this method. Saved configurations can be recalled from the list box at a future time.
- Click **Reset** to abandon any changes and return the gamma line to its original diagonal position.
- Click **OK** to save your changes and close the dialog box.
- Click **Cancel** to abandon your changes and close the dialog box.

Note: For best results, change the gamma while viewing a remote server.

The Message Board

The KVM over IP switch supports multiple user logins, which may cause access conflicts. To alleviate the problem, a message board has been provided, which allows users to communicate with each other:



Button Bar

The buttons on the Button Bar are toggles. Their actions are described in the table below:

Button	Action
	Enable/Disable Chat. When disabled, messages posted to the board are not displayed. The button is shadowed when Chat is disabled. The icon displays next to the user's name in the User List panel when the user has disabled Chat.
	Occupy/Release Keyboard/Video/Mouse. When you Occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. The button is shadowed when the KVM is occupied. The icon displays next to the user's name in the User List panel when the user has occupied the KVM.
	Occupy/Release Keyboard/Mouse. When you Occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed when the KM is occupied. The icon displays next to the user's name in the User List panel when the user has occupied the KM.
	Show/Hide User List. When you Hide the User List, the User List panel closes. The button is shadowed when the User List is open.

Message Display Panel

Messages that users post to the board - as well as system messages - display in this panel. If you disable Chat, however, messages that get posted to the board won't appear.

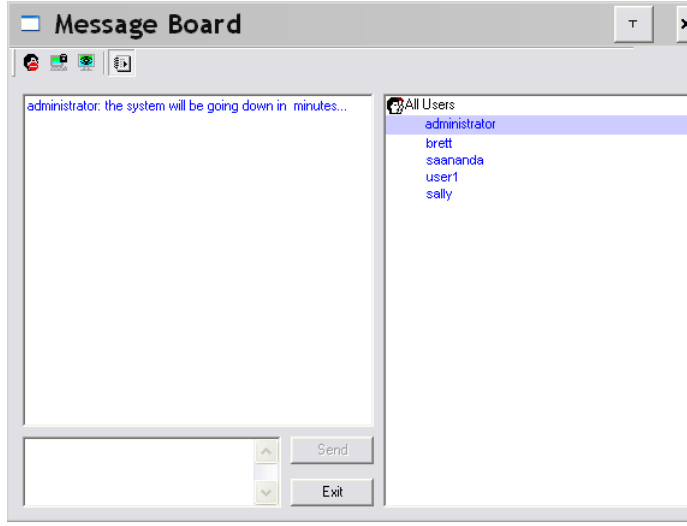
Compose Panel

Key in the messages that you want to post to the board in this panel. Click **Send**, or press [**Enter**] to post the message to the board.

User List Panel

The names of all the logged in users are listed in this panel.

- Your name appears in blue; other users' names appear in black.
- By default, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
- If a user's name is selected, and you want to post a message to all users, select All Users before sending your message.
- If a user has disabled Chat, its icon displays before the user's name to indicate so.
- If a user has occupied the KVM or the KM, its icon displays before the user's name to indicate so.



Virtual Media

The *Virtual Media* feature allows a drive, folder, image file, removable disk, or smart card reader on a user's system to appear and act as if it were installed on the remote server.

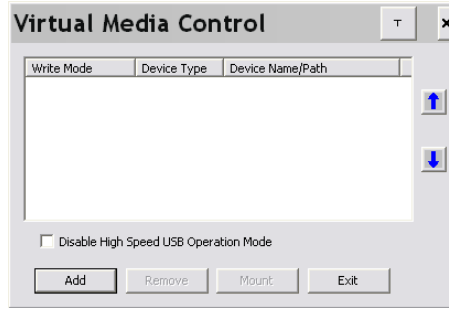
The Virtual Media icon changes depending on the status of the virtual media function, as shown in the table below:

Icon	Function
	The icon displays in gray to indicate that the virtual media function is disabled or not available
	The icon displays in blue to indicate that the virtual media function is available. Click the icon to bring up the virtual media dialog box.
	The icon displays in blue with a red **X** to indicate that a virtual media device has been mounted on the remote server. Click the icon to unmount all redirected devices.

Mounting Virtual Media

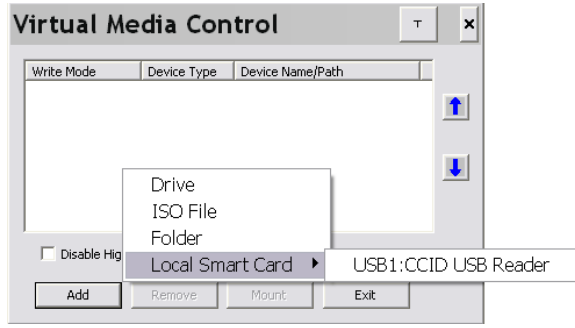
To mount a virtual media device, do the following:

1. Click the Virtual Media icon to bring up the *Virtual Media* dialog box:.



Note: The **T** button at the top right brings up a slider to adjust the transparency of the dialog box. After making your adjustment, click anywhere in the dialog box to dismiss the slider.

2. Click **Add**; then select the media source.

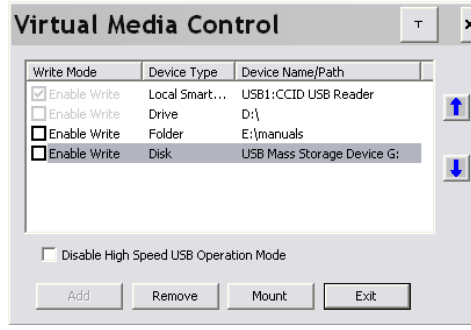


Depending on your selection, additional dialog boxes appear to enable you to select the drive, ISO file, folder, or removable disk you desire.
See *Virtual Media Support*, page 277 for a list of supported virtual media types, and details about mounting them.

3. If your device only supports full speed USB, put a check in the *Disable High Speed USB Operation Mode* checkbox.

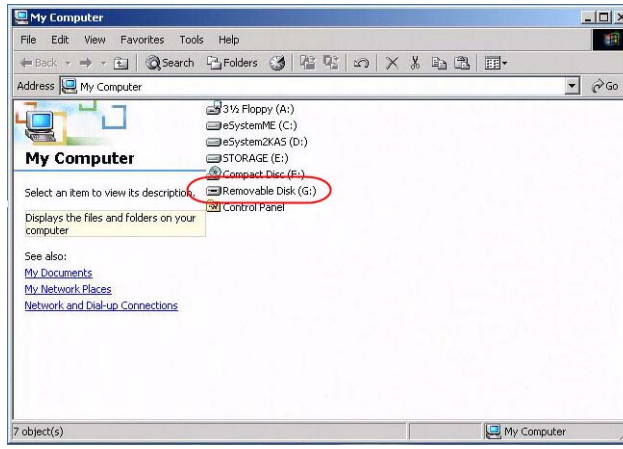
4. To add additional media sources, click **Add**, and select the source as many times as you require. Up to three virtual media choices can be mounted. The top three in the list are the ones that are selected. Virtual Media and Smart Card readers can be mounted at the same time. To rearrange the selection order, highlight the device you want to move, then click the Up or Down Arrow button to promote or demote it in the list.

5. *Read* refers to the redirected device being able to send data to the remote server; *Write* refers to the redirected device being able to have data from the remote server written to it. For the redirected device to be writable as well as readable, click to put a check in the *Enable Write* checkbox:



Note: If a redirected device cannot be written to, it appears in gray.

6. To remove an entry from the list, select it and click **Remove**.
7. After you have made your media source selections, click **Mount**. The dialog box closes. The virtual media devices that you have selected are redirected to the remote server, where they show up as drives, files, folders, etc. on the remote server's file system.



Once mounted, you can treat the virtual media as if they really existed on the remote server – drag and drop files to/from them; open files on the remote server for editing and save them to the redirected media, etc.

Files that you save to the redirected media will actually be saved on your local client computer's storage. Files that you drag from the redirected media will actually come from your local client computer's storage.

8. To end the redirection, bring up the *Control Panel* and click on the Virtual Media icon. All mounted devices are automatically unmounted.

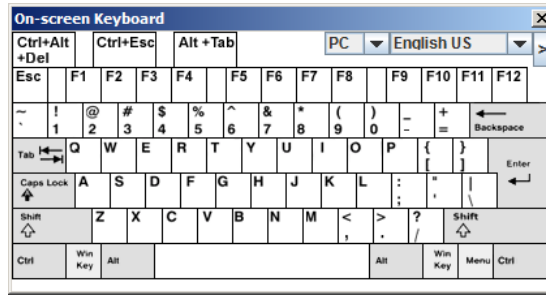
Zoom

The Zoom icon controls the zoom factor for the remote view window. Settings are as follows:

Setting	Description
100%	Sizes and displays the remote view window at 100%.
75%	Sizes and displays the remote view window at 75%.
50%	Sizes and displays the remote view window at 50%.
25%	Sizes and displays the remote view window at 25%.
1:1	Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents don't resize – they remain at the size they were. To see any objects that are outside of the viewing area move the mouse to the window edge, to have the screen scroll.

The On-Screen Keyboard

The KVM over IP switch supports an on-screen keyboard, available in multiple languages, with all the standard keys for each supported language. Click this icon to pop up the on-screen keyboard:



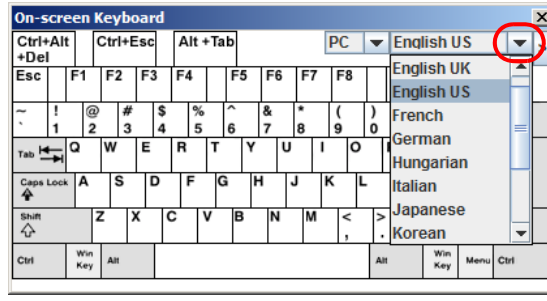
One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems aren't the same, you don't have to change the configuration settings for either system. Just bring up the on-screen keyboard; select the language used by the server you are accessing; and use the on-screen keyboard to communicate with it.

Note: You must use your mouse to click on the keys. You cannot use your actual keyboard.

Changing Languages

To change languages, do the following:

1. Click the down arrow next to the currently selected language, to drop down the language list.

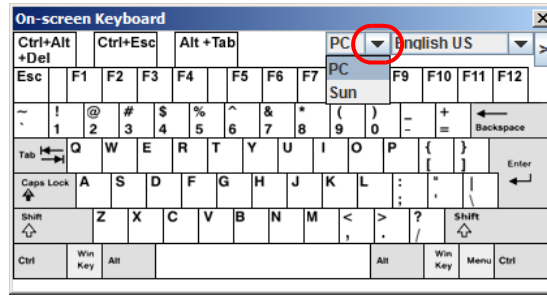


2. Select the new language from the list.

Selecting Platforms

The On-screen Keyboard supports the Sun platform as well as the PC. To select the platform, do the following:

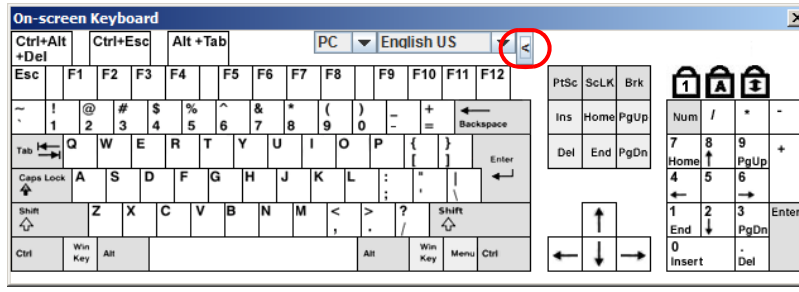
1. Click the down arrow next to the currently selected platform, to drop down the platform list.



2. Select the new platform from the list.

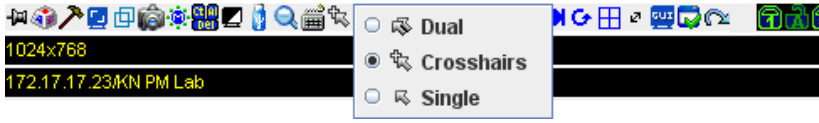
Expanded Keyboard

To display/hide the expanded keyboard keys, click the arrow to the right of the language list arrow.



Mouse Pointer Type

KVM over IP switches offer a number of mouse pointer options when working in the remote display. Click this icon to select from the available choices:



Note: 1. Before accessing a port, only Dual and Crosshairs are available for the Windows Viewers. Once the port is accessed, three pointers are available.

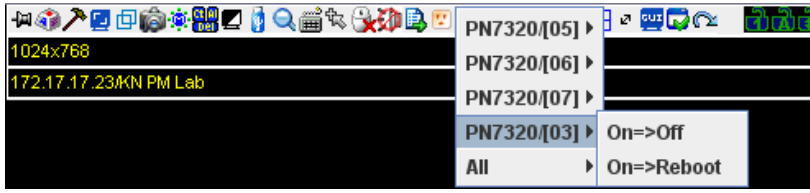
2. The Dot pointer is not available with the Java Client Viewer or the Java Client AP.

3. Selecting the Single pointer has the same effect as the *Toggle mouse display* hotkey function (see *Toggle mouse display*, page 65 for details).

4. The icon on the Control Panel changes to match your choice.

Power Over the Net™

The Power Over the Net™ icon provides the ability to power on, power off, and reboot outlets associated with the port on the PON device (see *Power Management*, page 130 for details) from the control panel. Click this icon to select from the available choices:



After clicking on the PON icon, a list of the power outlets associated with the connected port appears with the available options:

Options	Usage
On=>Off	Sends a Power Off signal to the selected outlet.
On=>Reboot	Sends a Reboot signal to the selected outlet.
Off=>On	Sends a Power On signal to the selected outlet.
All	Sends the selected signal (**On**, **Off**, **Reboot**) to all associated outlets.
Pending	A signal has been sent to the outlet and is in the process of performing the action.

Mouse DynaSync Mode

Synchronization of the local and remote mouse pointers is accomplished either automatically or manually.

Automatic Mouse Synchronization (DynaSync)

Mouse DynaSync provides automatic locked-in synching of the remote and local mouse pointers – eliminating the need to constantly resync the two movements.

Note: This feature is only available for Windows and Mac systems (G4 and higher) whose adapter attribute OS setting is configured for Win or Mac (see *Port Properties*, page 127), which are connected to the switch with one of the following Adapter Cables: KA7166, KA7168, KA7169, KA7170, KA7175, KA7176 or KA7177.

All other configurations must use manual mouse synchronization (described in the next section).

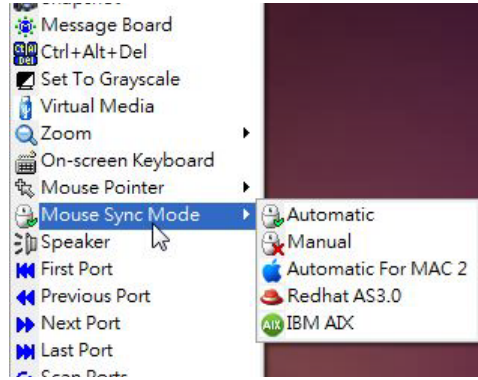
The icon on the Control Panel indicates the synchronization mode status as follows:

Icon	Function
	This icon displays in gray to indicate that Mouse DynaSync is not available – you must use manual synching procedures. This is the default setting for all KVM Adapters other than the KA7166, KA7168, KA7169, KA7170, KA7175, KA7176, and KA7177.
	The green check mark on this icon indicates that Mouse DynaSync is available and is **enabled**. This is the default setting when Mouse DynaSync is available. (See the Note, above.)
	The red X on this icon indicates that Mouse DynaSync is available but is **not enabled**.

When *Mouse DynaSync* is available, clicking the icon toggles its status between enabled and /disabled. If you choose to disable Mouse DynaSync mode, you must use the manual synching procedures described under *Manual Mouse Synchronization*, page 89.

Mac and Linux Considerations

- For Mac OS versions 10.4.11 and higher, there is a second DynaSync setting to choose from. If the default Mouse DynaSync result is not satisfactory, try the **Mac 2** setting. To select Mac 2, right click in the text area of the Control Panel and select *Mouse Sync Mode* → *Automatic for Mac 2*:



- Linux doesn't support DynaSync Mode, but there is a setting on the Mouse Sync Mode menu for Redhat AS3.0 systems. If you are using a USB Adapter Cable (see the Note on the previous page), with an AS3.0 system and the default mouse synchronization is not satisfactory, you can try the Redhat AS3.0 setting. In either case, you must perform the manual mouse synchronization procedures described in the next section.

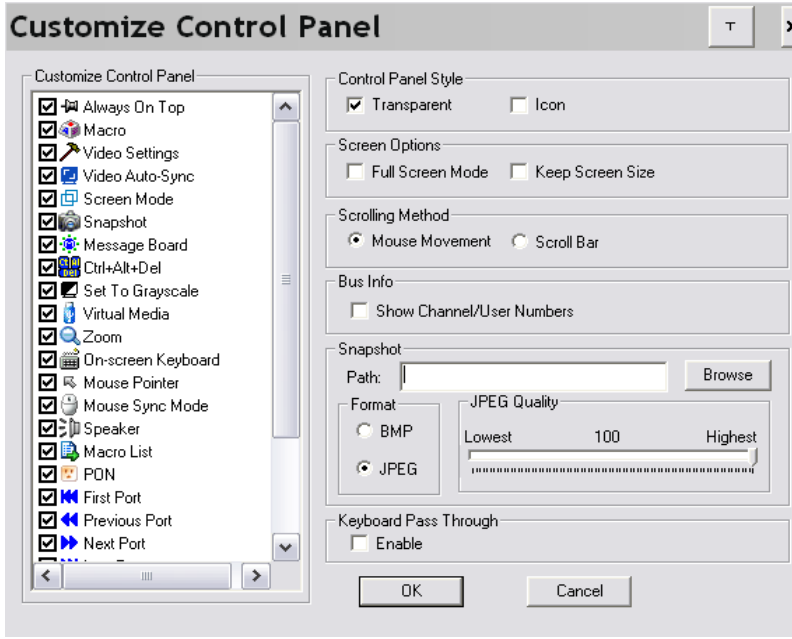
Manual Mouse Synchronization

If the local mouse pointer goes out of sync with the remote system's mouse pointer there are a number of methods to bring them back into sync:

1. Perform a video and mouse auto sync by clicking the *Video Settings* icon on the Control Panel (see page 73).
2. Perform an *Auto Sync* with the Video Adjustment function (see *Video Settings*, page 73, for details).
3. Invoke the *Adjust Mouse* function with the *Adjust Mouse* hotkeys (see *Adjust mouse*, page 65, for details).
4. Move the pointer into all 4 corners of the screen (in any order).
5. Drag the Control Panel to a different position on the screen.
6. Set the mouse speed and acceleration for each problematic server attached to the switch. See *Additional Mouse Synchronization Procedures*, page 265, for instructions.

Control Panel Configuration

Clicking the *Control Panel* icon brings up a dialog box that allows you to configure the items that appear on the Control Panel, as well as its graphical settings:



The organization of the dialog box is described in the table, below:

Item	Description
Customize Control Panel	Allows you to select which icons display in the Control Panel. Check the ones you want to see, uncheck the ones you don't want.
Control Panel Style	◆ Enabling *Transparent* makes the Control Panel semi-transparent, so that you can see through it to the display underneath. ◆ Enabling *Icon* causes the Control Panel to display as an icon until you mouse over it. When you mouse over the icon, the full panel comes up.

Item	Description
Screen Options	◆ If *Full Screen Mode* is enabled, the remote display fills the entire screen. ◆ If *Full Screen Mode* is not enabled, the remote display appears as a window on the local desktop. If the remote screen is larger than what is able to fit in the window, move the mouse pointer to the screen border that is closest to the area you want to view and the screen will scroll. ◆ If *Keep Screen Size* is enabled, the remote screen is not resized. ◆ If the remote resolution is smaller than that of the local monitor, its display appears like a window centered on the screen. ◆ If the remote resolution is larger than that of the local monitor, its display is centered on the screen. To access the areas that are off screen, move the mouse to the corner of the screen that is closest to the area you want to view and the screen will scroll. ◆ If *Keep Screen Size* is not enabled, the remote screen is resized to fit the local monitor's resolution.
Scrolling Method	In cases where the remote screen display is larger than your monitor, you can choose how to scroll to the areas that are off-screen. ◆ If you select *Mouse Movement*, the screen will scroll when you move the mouse pointer to your screen border. ◆ If you select *Scroll Bars*, scroll bars appear around the screen borders that you can use to scroll to the off-screen areas.
Bus Info	If *Bus Info* is enabled, the number of the bus you are on, as well as the total number of users on the bus, displays on the bottom row center of the Control Panel as follows: Bus No./Total Users. (See the Control Panel diagram on page 59 for an example.)
Snapshot	These settings let the user configure the KVM over IP switch's screen capture parameters (see the *Snapshot* description under *The Control Panel*, page 59): ◆ Path lets you select a directory that the captured screens automatically get saved to. Click **Browse**; navigate to the directory of your choice; then click **OK**. If you don't specify a directory here, the snapshot is saved to your desktop. ◆ Click a radio button to choose whether you want the captured screen to be saved as a BMP or a JPEG (JPG) file. ◆ If you choose JPEG, you can select the quality of the captured file with the slider bar. The higher the quality, the better looking the image, but the larger the file size.
Keyboard Pass Through	When this is enabled, the Alt-Tab key press is passed to the remote server and affects that server. If it is not enabled, Alt-Tab acts on your local client computer.

The Java Control Panel

The Java Client Viewer and Java Client AP Control Panel is similar to the one used by the WinClient:

The major differences between them are:

- In the Macros dialog box, *Toggle Mouse Display* is not available.
- The *Dot* mouse pointer type is not available.
- In the Message Board, there is no *Show/ Hide* button to show or hide the user list. This function is achieved by clicking the arrows at the top of the bar that separates the User List panel from the Main panel.

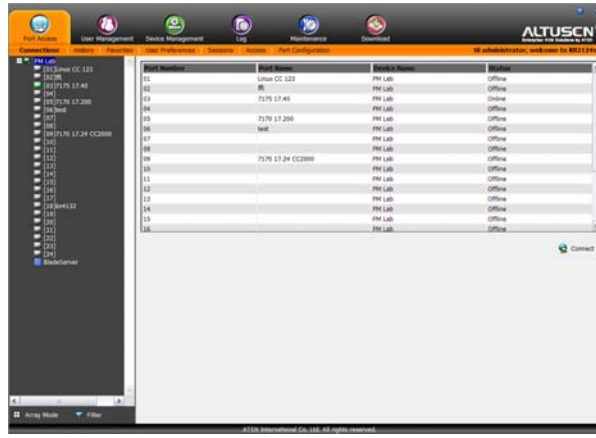
- In Virtual Media, only ISO and Folder are supported. See *Java Client Viewer / Java Client AP*, page 277 for further details.
- The Control Panel *Lock LED* icons are not in sync with your keyboard. When you first connect, the LED display may not be accurate. To be sure, click on the LED icons to set them.
- In *Control Panel Configuration*, the BMP Snapshot format has been replaced by PNG.

Chapter 6
Port Access

Overview

When you log in to the switch the *Port Access* page comes up with the KVM over IP switch's KVM *Connections* page displayed.

Browser GUI



AP GUI

The Connections page is organized into several main areas. All the devices, ports, and outlets that a user is permitted to access are listed in the Sidebar at the left of the page. In addition to KVM over IP device listings, if any PON (Power Over the Net™) devices are connected to the switches they are listed separately below the switch listings. If any Blade Servers have been deployed, they are listed separately below the PON devices.

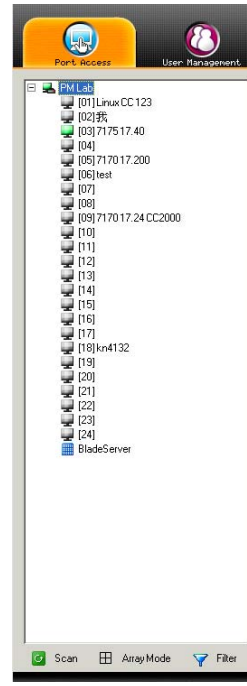
Configuration and operation of KVM devices and ports are discussed on page 101; configuration and operation of PON devices and outlets are discussed on page 104; configuration and operation of Blade Servers are discussed on page 109

Note: Power Over the Net™ devices are also referred to as PDUs (Power Device Units).

After selecting a device, port, or outlet in the Sidebar, clicking entries on the menu bar (Browser GUI) or tab bar (AP GUI) opens information and configuration pages related to the item selected in the Sidebar.

The Sidebar

All KVM switches, PON devices, and Blade Servers – including their ports and outlets – are listed in a tree structure in the Sidebar at the left of the screen:



The Sidebar Tree Structure

The characteristics of the Sidebar tree structure are the following:

- Users are only allowed to see the devices and ports/outlets that they have access permission for.
- Ports/outlets and child devices can be nested under their parent devices.

  Click the + in front of a device to expand the tree and see the ports/outlets nested underneath it. Click the - to collapse the tree and hide the nested ports/outlets.
- A port's/outlet's ID number is displayed in brackets next to its icon. The ports/outlets but can also be named (see *Port/Outlet Naming*, page 99, for details).
- Switches and ports that are on line have their monitor screen icons in Green; the monitor screens are Gray for devices and ports that are offline.

- Outlets that are *On* have their icons in Amber; the icons are Gray for outlets that are *Off*.
- To access and operate a port, double click its icon. Port operation details are discussed in Chapter 12, *Port Operation*.

Note: 1. In the Browser version, you can open as many port viewers as there are ports, but the number of ports that you see depends on the number of buses that the switch supports. For example, if the switch supports 4 buses, the 5th viewer displays the same port as the 1st viewer; the 6th viewer displays the same screen as the 2nd viewer, etc.
In the AP GUI version you can only access one port at a time. To see two different ports, you would have to log in two separate times.

2. If the *CC Management* function is enabled (see page 168), PON devices and Blade Servers do not appear in the Sidebar, even if they are configured on the switch. This is because they are managed via the CC server.

Scan

Scan is found at the bottom of the AP GUI Sidebar. It automatically switches among all the ports that are visible in the Sidebar (see Filter, below), at regular intervals, so that their activity can be monitored automatically. See *Auto Scanning*, page 213 for details.

Note: This item doesn't appear at the bottom of the Sidebar in the Browser version. In that version, you must invoke it from the port's *Toolbar*. See *The Port Toolbar*, page 211 for details

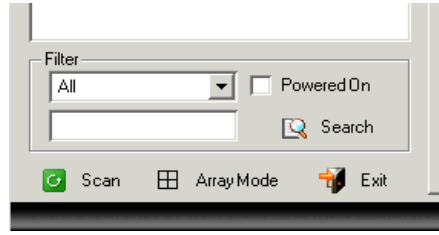
Array

Array is found at the bottom of the AP GUI Sidebar. It represents another way of monitoring port activity. Under this function your screen is divided into a grid of panels, with each panel showing the video display of a particular port. Only ports that are visible in the Sidebar (see Filter, below), and that are on line are displayed – all other ports are blank. See *Panel Array Mode*, page 216 for details

Note: This item doesn't appear at the bottom of the Sidebar in the Browser version. In that version, you must invoke it from the port's *Toolbar*. See *The Port Toolbar*, page 211 for details

Filter

Filter allows you to control the number and type of ports that display in the Sidebar, as well as which ports get scanned when Auto Scan and Array Modes are invoked (see *Scan* and *Array*, above). When you click *Filter*, the bottom of the panel changes to look similar to the image, below:

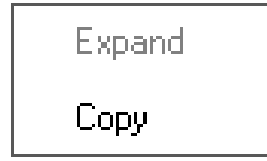


The meanings of the choices are explained in the following table:

Choices	Explanation
All	This is the default view. With no other filter options selected, all of the ports that are accessible to the user are listed in the Sidebar. If any *Favorites* have been specified (see page 114), you can drop down the list box and select Favorites instead of All. If you select Favorites, only the items you have selected as Favorites display in the tree.
Powered On	If you enable *Powered On* (by putting a check in the checkbox) only the ports that have their attached devices powered on display in the tree.
Search	If you key in a search string and click **Search**, only port names that match the search string display in the tree. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported, so that more than one port can show up in the list. For example: 1. If you key in **Web***, both Web Server 1 and Web Server 2 show up in the list. 2. If you key in **W*1 or M*2**, both Web Server 1 and Mail Server 2 show up in the list.
Exit	Clicking **Exit** closes the filter dialog.

Sidebar Utilities

The AP GUI version Port Access *Connections* page provides a convenient method to work with the Sidebar tree. When you right click an item, a list with various options pops up:



Note: The screenshot shows an example of just one of the pop-ups that can appear. The items that appear in the pop-up depend on whether you are logged in remotely or from a Local Console; what your user type is; and whether you selected a switch or a port.

The following table lists and explains all of the possible items that may appear:

Item	User Type	Explanation
Expand/ Collapse	Administrators Users	◆ If the device's ports are nested (not displayed), the dialog box entry is *Expand*. Click **Expand** to display the nested ports. ◆ If the device's ports are displayed, the dialog box entry is *Collapse*. Click **Collapse** to nest the ports. **Note:** 1. This item only appears for switches, or for ports that have child devices connected to them. 2. This has the same effect as clicking the **+** or **-** in the tree structure.
Copy	Administrators Users	This item is only available for ports. After selecting Copy, you can Paste the port into the Favorites page. See *Adding a Favorite*, page 114 for details

Port/Outlet Naming

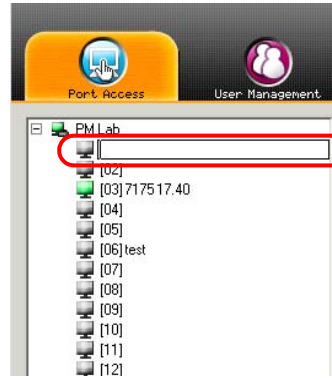
For convenience – especially in large installations with many devices, ports and outlets – administrators and users with port configuration permission, can give each port or outlet a name. To assign, modify or delete a name, do the following:

1. Click once on the item you want to edit; wait a second; then click again.

Note: 1. This is not a double click. It involves two separate clicks. A double click will switch you to the device attached to the port.

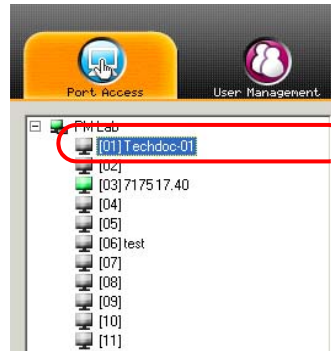
2. In the AP GUI version you can right click on the port you want to edit, then select **Rename** in the popup box that appears, or you can highlight the port and press **F2**.

After a second or two, the field changes to provide a text input box:



2. Key in a name for the item (or change/delete a previous one).
   - You can use any combination of letters, numbers, and symbols on the typewriter keys of keyboards with PC US English layout. In this case, the maximum number of characters allowed is 20.
   - You can also activate your local IME to input non-English characters. For languages that use 2 byte encoding, the maximum number of characters allowed is 9.

3. When you have finished editing the name, press **[Enter]** or click anywhere outside of the input box to complete the operation.



KVM Devices and Ports – Connections Page

For KVM over IP switches, the *Connections* page displays port status information at the device level, and port connection configuration options at the port level.

Device Level

When a KVM over IP switch is selected in the Sidebar, the Connections page displays a list of ports for the device that the user is authorized to access or view.

The following attributes are listed for each device:

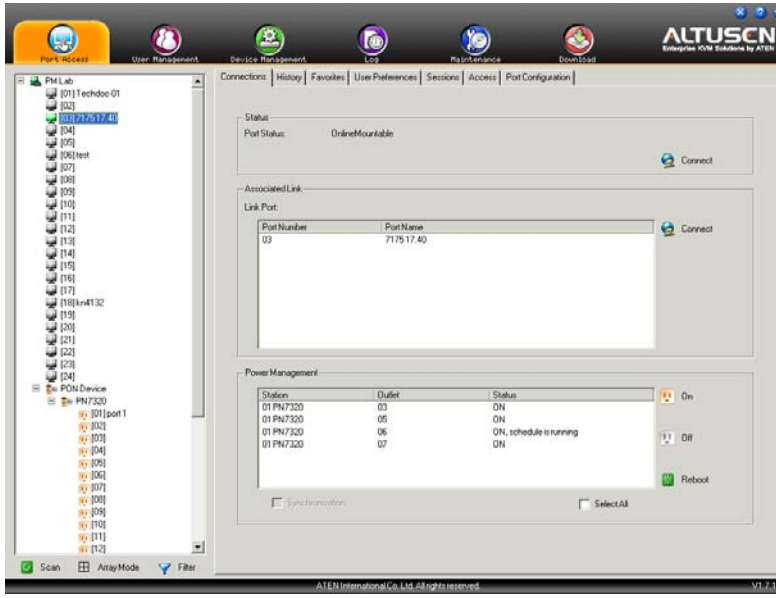
- Port Number – the port's number on the switch.
- Port Name – if a name has been assigned to a port it displays here.
- Device Name – if a name has been assigned to the switch it displays here.
- Status – the current status of the port – online, or offline.

Note: The sort order of the information displayed can be changed by clicking the column headings.

You can access a port from the main panel either by double clicking anywhere on its line entry, or selecting it anywhere on its line entry and clicking **Connect** at the bottom right of the page.

Port Level

When a port is selected in the Sidebar, the *Connections* page changes to display the port connection and configuration options:



The screen is divided into three major panels, as described in the sections that follow.

Status

The Status Panel displays the port's current status information, including whether the port is online or offline, and if the port is mountable.

Click the **Connect** button to view the port display via the switch's built-in Win Viewer (when using Windows Internet Explorer), or Java Viewer (when using other web browsers).

Associated Links

The Associated Links panel displays ports that have been associated with the currently selected port. Associations are configured on the *Port Access* → *Port Configuration* → *Associated Links* page (see page 129 for details).

Power Management

If a PN0108 is connected to the KVM over IP switch, and a device is connected to one of the PN0108's outlets, you can power manage (On, Off, Reboot) selected outlets directly from this page, instead of having to select them on the PON device, itself.

Associating outlets with a port is accomplished on the *Port Access → Port Configuration → Power Management* page (see page 130 for details).

- If there is more than one outlet associated with this port, click on the line entry to select the one you want to manage, then click the **On**, **Off**, or **Reboot** icon, as appropriate.

Note: For the Reboot option, the outlet must be configured with *System After AC Back* or *Modem Ring Resume* as its operating mode.

- If there is more than one outlet associated with this port, and you want to power manage several of them at once, use *Shift-Click* (for a sequential set), or *Ctrl-Click* (for a non-sequential set) to select your group.
- If there is more than one outlet associated with this port, and you want to power manage all of them at once, click to put a checkmark in the *Select All* checkbox.

Note: 1. Even though the outlets all turn On, Off, or Reboot at the same time, they do so with their own separate outlet configuration settings (delay, operating mode, etc. See *Port Configuration*, page 126 for details).

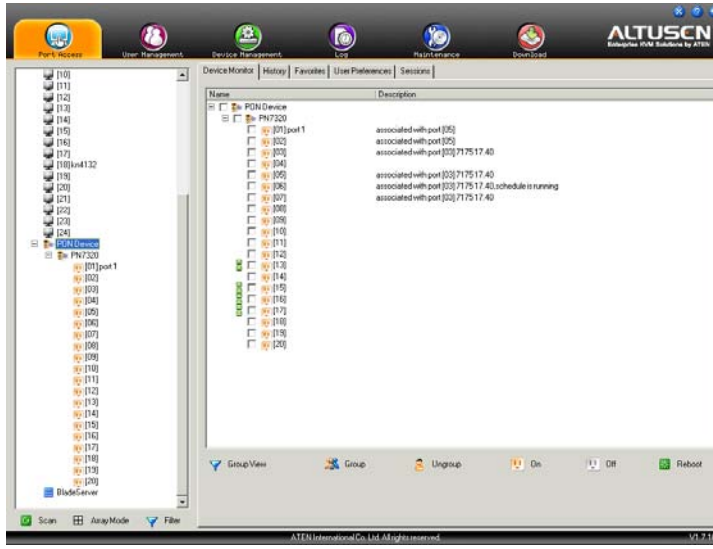
2. For the Reboot option, the outlet must be configured with *System After AC Back* or *Modem Ring Resume* as its operating mode.

- The *Synchronization* checkbox is read only. Whether it is enabled or not is set on the *Port Configuration → Power Management* page (see page 126). When Synchronization is enabled, the outlets on devices with more than one power supply can all be operated at the same time.

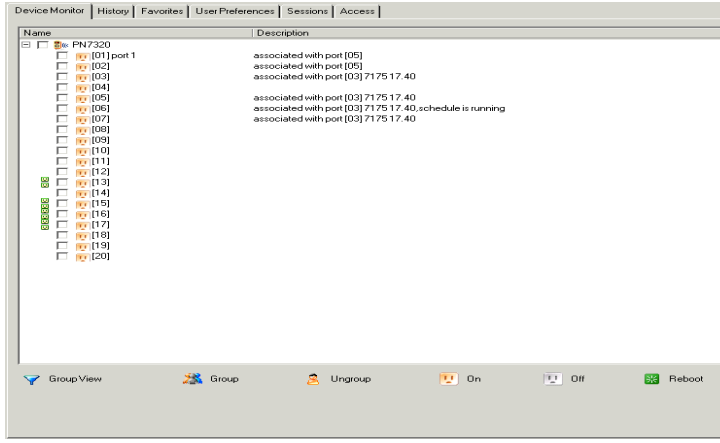
Note: For the Reboot option, the outlets must be configured with *System After AC Back* as the operating mode.

PON Devices – Device Monitor Page

Power Over the Net™ (PON) devices that are connected to the switches display below the KVM switches in the Sidebar. When a PON device is selected in the Sidebar, the *Device Monitor* page appears:



The Main Panel – PON View



PON View is the default page view, All PON devices and their outlets that are connected to the switch are listed under the *Name* column.

Outlets that are synchronized or that belong to groups have a green power outlet icon in front of their names. Click an outlet's green icon to display which other outlets it synchronizes with, or is grouped with. Click the green outlet again to close the information display,

The *Description* column displays which KVM port the outlet is associated with.

Action Buttons

The actions that the buttons at the bottom of the page perform are described in the table below:

Button	Action
Group View	Click this button to switch the display to *Group View* – see *The Main Panel – Group View*, page 107 for details.
Group	Select the outlets that you want to form into a group, then click this button to create it (see *Outlet Groups*, page 106 for details).
Ungroup	Select the outlets that you want to remove from a group, then click this button to remove them
On	Sends a Power On signal to the selected outlet(s).
Off	Sends a Power Off signal to the selected outlet(s).
Reboot	Sends a Reboot signal to the selected outlet(s).

Outlet Groups

To create outlet groups, do the following:

1. Select the outlets you want to include in the group.
2. Click **Group**.

   The Outlet Group dialog box comes up:

3. Select whether or not the outlets will belong to a new group or to an existing group.

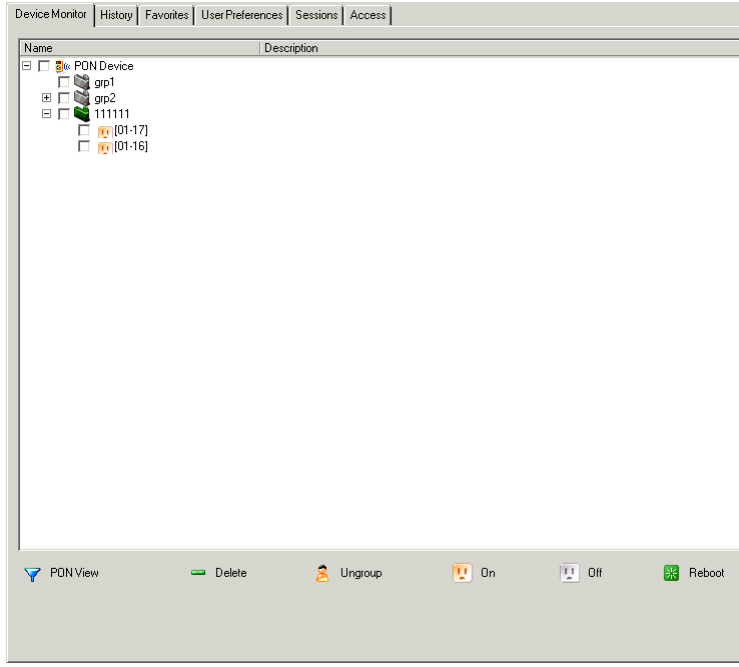
   a) If it is a new group, give it a name in the text field.

   b) If it is an existing group, select the group in the central panel.

4. Click **Save**.

To remove outlets from groups, select them in the main panel, then click **Ungroup**.

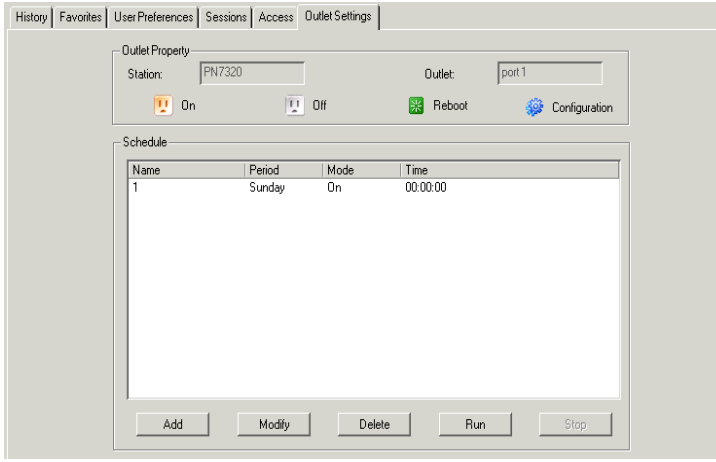
The Main Panel – Group View



- Clicking the PON View button takes you back to the PON View page.
- To delete a group, select it in the main panel, then click **Delete**.
- Selecting a group in the main panel, then clicking **Ungroup**, removes all outlets from that group. It provides a shortcut method to remove all of them at once, rather than having to remove then one by one from the PON View page.
- To power manage a group of outlets, first select the group(s) in the main panel, then click the appropriate power button.

Outlet Settings

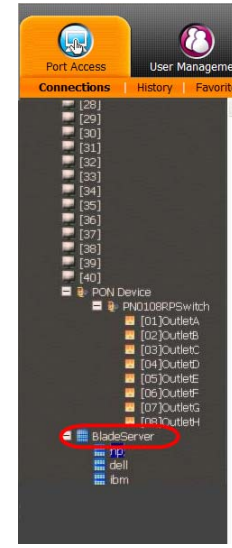
When an outlet is selected in the Port Access page Sidebar, the *Outlet Settings* page appears:



- The *Outlet Properties* panel indicates the name of the PON that the outlet belongs to and the outlet's name, as well as On, Off, Reboot, and Configuration buttons to manually manage the outlet's power.
- The *Schedule* panel lets you set up an automated Power management configuration for the outlet. The procedure for accomplishing this is the same as the one described in the *Power Management* section. See *Schedule*, page 133 for details.

Blade Servers – Connections Page

Blade Servers that are connected to the switches display below the KVM switches and PON devices in the Sidebar.



This section describes accessing and configuring the blade servers, and associating the blades with KVM switch ports. By associating a blade server or blade with a port the servers and blades are integrated into the Sidebar tree view, and appear as devices connected to the port.

The Blade Configuration Page

The *Blade Configuration* page is where the associations between the blade servers and the KVM switch ports get made. To access this page, select the blade server or blade then click *Blade Configuration (*the menu item at the far right of the menu bar).

For IBM and Dell blade servers, the entire chassis gets associated with a port, and each blade in the chassis will appear in the tree as a child port of the associated port – as in port 08 in the screenshot at the right.

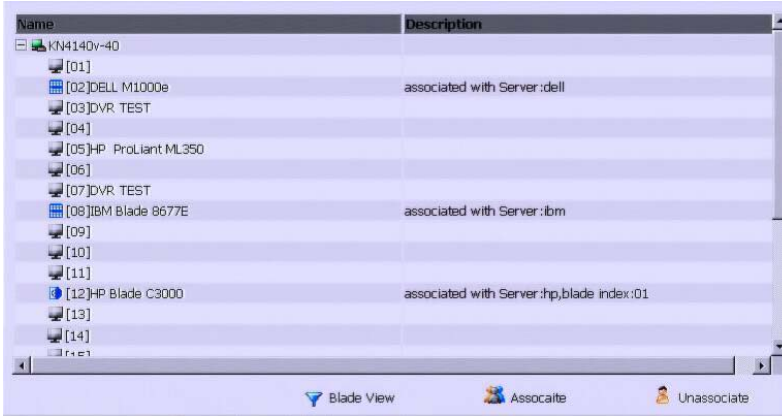
For HP blade servers, associations are made on a blade by blade basis. Each blade is associated with a single port.

To access a blade, click on its port entry in the tree.

Associating Ports

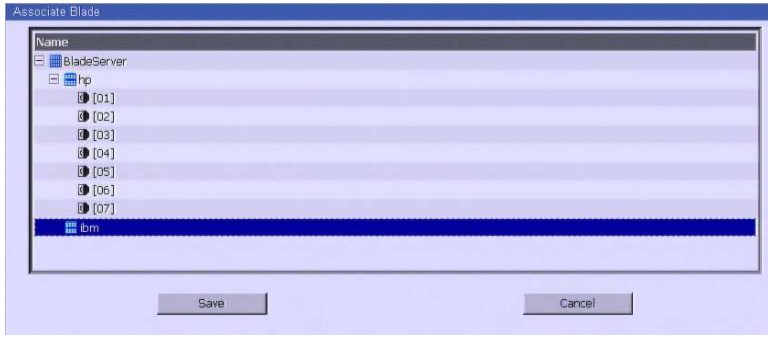
Main Panel Device View

Port association begins by clicking the Blade Configuration menu item at the far right of the menu bar. The page comes up in *Device View*, listing all of the KVM switch's ports, and the blade servers (IBM and Dell servers), or individual blades (HP servers) that have been associated with them:



To make an association from the device view, you first select a KVM port, then select a blade server or blade to associate it with as follows:

1. Select the port in the main panel
2. Click **Associate**
3. In the screen that comes up, select the blade server or individual blade that you want to associate with the selected port.



4. Click **Save**.

After the association completes successfully, the *blade icon* appears as the port indicator in the Sidebar tree. To access the device running on the blade, click on its entry in the Sidebar.

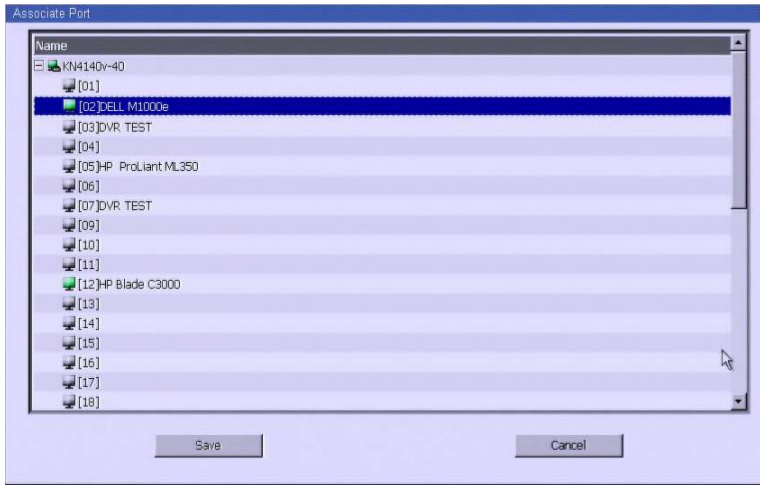
Main Panel Blade View

At the bottom of the Device View main panel is a button labeled *Blade View*. This is a button that toggles the main panel between the two views. Click it to bring up the main panel in Blade View:

Blade View lists all of the blade servers (IBM and Dell servers) and individual blades (HP servers) that are installed on the system, and the ports (if any) that they are associated with.
To make an association from the blade view, you first select a blade server or blade, then select a KVM port to associate it with as follows:

1. Select the blade server or blade in the main panel.
2. Click **Associate** (at the bottom of the main panel).

3. In the screen that comes up, select the port that you want to associate it with.



4. Click **Save**.

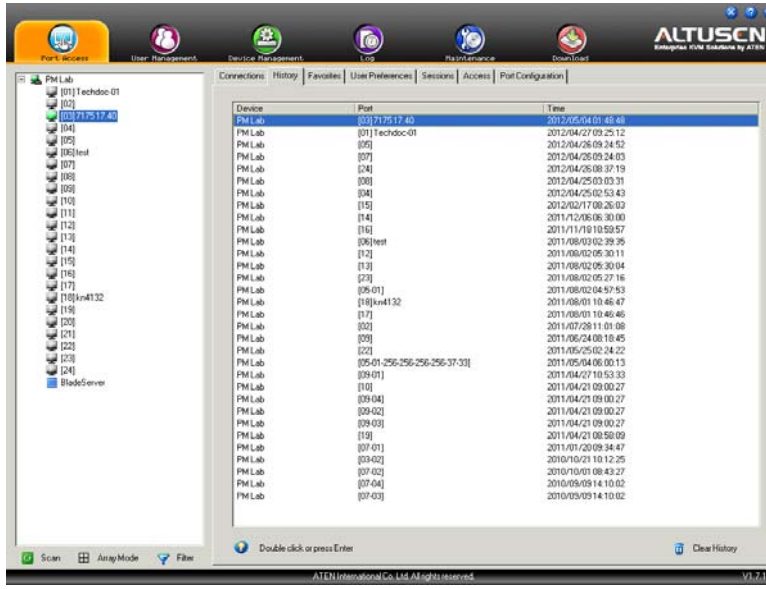
After the association completes successfully, the *blade icon* appears as the port indicator in the Sidebar tree. To access the device running on the blade, click on its entry in the Sidebar.

Unassociating Ports

To break the association between a port and a blade server or individual blade, select the association in the main panel, then click **Unassociate**.

History

The History page provides a record of each time that a port was accessed. It provides quick access to the most recently used ports. You can access a port shown in the main panel by double clicking it.



- If there are more entries than there is room on the screen, a scroll bar appears to let you scroll up and down to see the entire record.
- To clear the record and start over, click the *Clear History* button at the bottom right of the page.

Note: You can change the sort order of the information displayed by clicking the column headings.

Favorites

The *Favorites* page is similar to a bookmarks feature. Ports that you frequently access can be saved in a list here. Simply open this page and select the port – rather than hunting for it in the Sidebar. This feature is especially handy on large, crowded installations:

Adding a Favorite

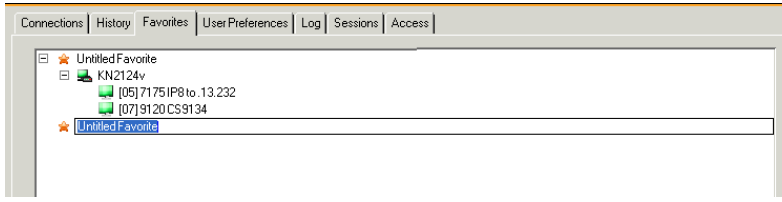
To add a port to the favorites, do the following:

1. Right click in the main panel; click **Add Favorite**.

   – or –

   Click **Add** at the bottom left of the main panel.

   An *Untitled Favorite* entry appears:



2. This will be a container to hold your port entries. Click inside the text entry box to erase *Untitled Favorite* and key in an appropriate name, then click on any empty space in the main panel.

3. To add a port:

   Drag it from the Sidebar and drop it onto the container

   – or –

   Right Click on it in the Sidebar; select **Copy**. Right click on the container; select **Paste**.

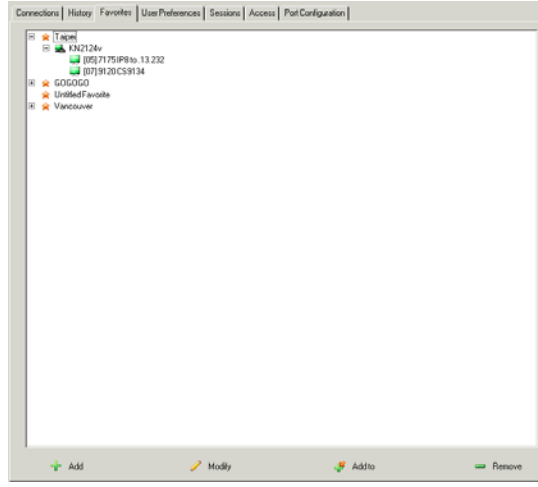
   – or –

   Select the container in the main panel; select the port in the Sidebar; then click **Add to** at the bottom of the main panel.

   The switch that the port belongs to is added to the container; the selected port is appended under the switch.

   Note: To add multiple ports at the same time, hold the Shift or Ctrl key down while you make your Sidebar selections then drag or copy the entire group to the Favorites panel.

4. Repeat step 3 for any other *Favorite* categories you wish to create



Note: Favorites can be selected for filtering in the Sidebar. See *Filter*, page 97 for details

Modifying a Favorite

- To modify a Favorite, or one of the items contained in it, right click on it, then select a choice from the popup menu that appears.
- To edit a Favorite's name:

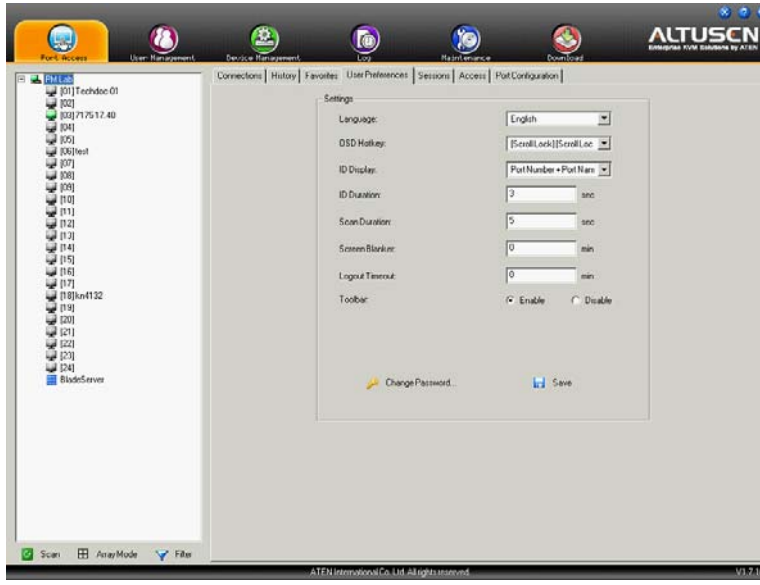
  Click on it once, wait a second, then click again. You can edit the name after the display changes to provide a text input box, This is the same procedure as the one described for port naming (see *Port/Outlet Naming*, page 99).

  – or –

  Select the Favorite in the main panel, then click **Modify** at the bottom of the main panel.

User Preferences

The *User Preferences* page allows users to set up their own, individual, working environments. The switch stores a separate configuration record for each user profile, and sets up the working configuration according to the *Username* that was keyed into the Login dialog box:



The page settings are explained in the following table:

Setting	Function
Language	Selects the language that the interface displays in.
OSD Hotkey	Selects which Hotkey controls the GUI function: [Scroll Lock] [Scroll Lock] is the default. To select a different combination, click the arrow at the right of the box to drop down the list of choices.
ID Display	Selects how the Port ID is displayed: the Port Number alone (PORT NUMBER); the Port Name alone (PORT NAME); or the Port Number plus the Port Name (PORT NUMBER + PORT NAME). The default is PORT NUMBER + PORT NAME.
ID Duration	Determines how long a Port ID displays on the monitor after a port change has taken place. You can choose an amount from 1—255 seconds. The default is 3 Seconds. A setting of 0 (zero) means the Port ID is always on.

Setting	Function
Scan Duration	Determines how long the focus dwells on each port as it cycles through the selected ports in Auto Scan Mode (see *Auto Scanning*, page 213). Key in a value from 1—255 seconds. The default is 5 seconds; a setting of 0 disables the Scan function.
Screen Blanker	If there is no input from the console for the amount of time set with this function, the screen is blanked. Key in a value from 1—30 minutes. A setting of 0 disables this function. The default is 0 (disabled). **Note:** Although this function can be set from either the local console or a remote login, it only affects the local console monitor.
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out. A login is necessary before the KVM over IP switch can be accessed again.
Toolbar	Selects whether or not the Port Toolbar is enabled when a port is accessed (see *The Port Toolbar*, page 211 for details). Since the Toolbar functions are also available from the GUI Control Panel (see *The Control Panel*, page 59), you may prefer to disable it here.
Viewer*	You can choose which viewer is used when accessing a server: ◆ **Auto Detect** will select the appropriate viewer based on the web browser used; WinClient for Windows Internet Explorer, Java Client for other web browsers (ex. Firefox). ◆ **Java Client** will open the Java based viewer regardless of the web browser being used.
Welcome Message*	You can choose to hide or show the welcome message displayed in the submenu bar. The default is disabled.
Save	Click **Save** to save any changes made to the User Preferences settings.
Changing a Password	◆ In the Browser GUI, to change a user's password, key in the old password and new password into their input boxes; key the new password into the *Confirm* input box, then click **Change Password** to apply the change. ◆ In the AP GUI version, click **Change Password**; key in the old password and new password into their input boxes; key the new password into the *Confirm* input box, then click **Save**.

***** This item is only available with the Browser version.

Sessions

The *Session* page lets the administrator and users with User Management permissions see at a glance which users are currently logged into the KVM over IP switch, and provides information about each of their sessions.

Note: 1. The Session page isn't available for ordinary users.

2. Users with User Management permissions can only see the sessions of ordinary users
3. The *Category* heading lists the type of user who has logged in: SA (Super Administrator); Admin (Administrator); Normal user (User).

The meanings of the headings at the top of the page are fairly straightforward. The *IP* heading refers to the IP address that the user has logged in from; the *Device* and *Port* headings show which device and port the user is currently accessing. The *Bus ID* refers to the bus that the user is currently on (Bus 0 refers to the Local Console's bus).

Note: 1. The sort order of the information displayed can be changed by clicking the column headings.

2. The Bus ID also displays on the control panel (see page 59). See *Users and Buses*, page 219 for information about buses.

This page also gives the administrator the option of forcing a user logout by selecting the user and clicking **End Session** at the bottom of the main panel.

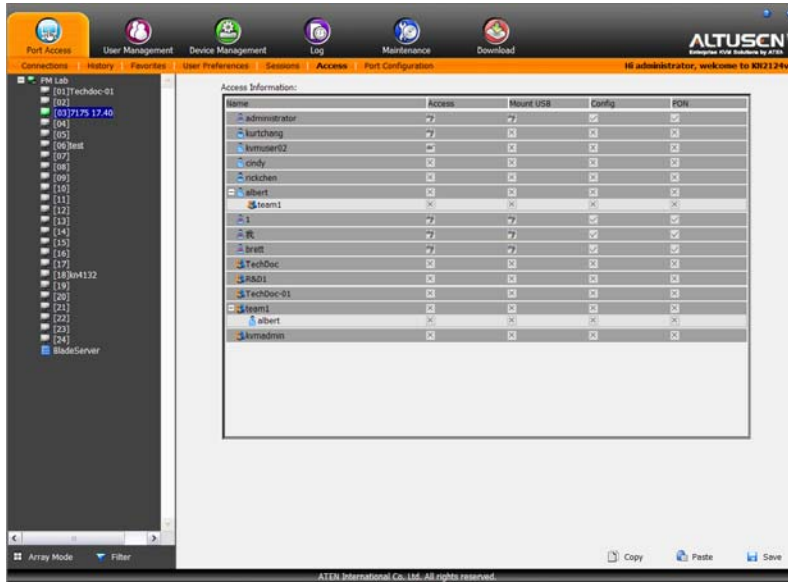
Access

Administrators use the *Access* page to set user and group access and configuration rights for switches and ports.

Note: The Access page only appears for those users with User Management permissions. It isn't available for other users.

Device Level Browser GUI Interface

If a switch is chosen in the Sidebar, the Main panel looks similar to the one shown below:



The main panel consists of two columns: *Name*, and *Config*:

- *Name* lists all the users and groups that have been created.
- *Config* indicates the users who have Configuration privileges. A check mark (√) indicates that the user has permission to make changes to the switch configuration settings (see Chapter 8, *Device Management*); an X means that the user is denied permission to make configuration changes. Click the icon to toggle permission for Administrators and Users (Super Administrators always have configuration privileges).

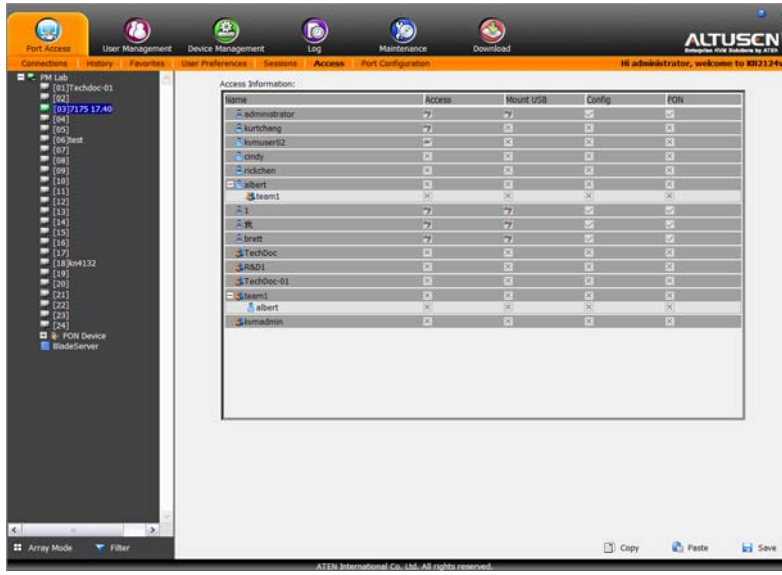
- The *Copy* and *Paste* buttons at the bottom of the main panel provide a shortcut method of assigning the permissions settings of one port to any of the other ports. To do so:

  1. Select the port whose permissions you want the other port(s) to follow.
  2. Click **Copy**.
  3. Select the port you want to receive the permissions.
  4. Click **Paste**.

- When you have finished making your configuration changes, click **Save**.

Port Level Browser GUI Interface

If a port is chosen in the Sidebar, the Main panel looks similar to the one shown below:



The port access settings are explained in the following table:

<table>
<tr><td>Name</td><td colspan="3">Each port accessible to the user is listed under the Names column.</td></tr>
<tr><td>Access</td><td colspan="3">The Access column is where device access rights are set. To cycle through the choices, click the icon in the row that corresponds to the user you want to configure. The meanings of the icons are as follows</td></tr>
<tr><td></td><td> </td><td>Full Access</td><td>The user can view the remote screen and can perform operations on the remote server from his keyboard and monitor.</td></tr>
<tr><td></td><td> </td><td>View Only</td><td>The user can only view the remote screen; he cannot perform any operations on it.</td></tr>
<tr><td></td><td> </td><td>No Access</td><td>No access rights - the Port will not show up on the User's list on the Main Screen.</td></tr>
<tr><td>Mount USB</td><td colspan="3">The Mount USB column is where permission to mount Virtual Media devices on remote servers is configured. To cycle through the choices, click the icon in the row that corresponds to the user you want to configure. The icons are the same as the ones in the Access column.
◆ With a Full Access setting, the user can mount, read, and write to the virtual media.
◆ With a View Only setting, the user can only view the contents of the virtual media (read only), he can not perform any operations on it.
◆ With a No Access setting, the user will not see the virtual media even if it has been configured on the remote system.
Note: This entry does not appear for switches that do not support the USB Virtual Media function.</td></tr>
<tr><td>Config</td><td colspan="3">Sets or denies permission for the user to make changes to a port's configuration settings. A check mark (√) indicates that the user has permission; an X means that the user does not have permission.</td></tr>
<tr><td>PON</td><td colspan="3">The PON column permits/restricts the configuration and power operation of ports that have Power Over the Net™ devices connected to them. A check mark (√) indicates that the user has permission; an X means that the user does not have permission.</td></tr>
</table>

Device Level AP GUI Interface

If a switch is chosen in the Sidebar, the Main panel looks similar to the one below:

The page is essentially the same as the one for the Browser GUI (see page 120), with the exception that there are filters at the top of the columns. The filters allow you to expand or limit the scope of the users and groups that are displayed, as described in the following table:

Filter		Description
Name		To filter on the User or Group name, key in the name, partial name or partial name, then press **Enter**. Only the Users and Groups whose names correspond to what you have keyed in appear in the list. Wildcards (? for single characters; * for multiple characters) and the keyword "or" are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
Config	All	All Users and Groups appear in the list.
	Permitted	Only Users and Groups with configuration permissions appear in the list.
	Restricted	Only Users and Groups that do not have configuration permissions appear in the list.

Port Level AP GUI Interface

If a port is chosen in the Sidebar, the Main panel looks similar to the one below:

The page is essentially the same as the one for the Browser GUI (see page 121), with the exception that there are filters at the top of the columns. The filters allow you to expand or limit the scope of the users and groups that are displayed, as described in the following table:

Filter		Description
Name		To filter on the User or Group name, key in the name, partial name, or partial name and wild card (*) then press **Enter**. Only the Users and Groups whose names correspond to what you have keyed in appear in the list.
Access	All	All Users and Groups appear in the list.
	Full Access	Only Users and Groups with Full Access permissions appear in the list.
	View Only	Only Users and Groups with View Only permissions appear in the list.
	No Access	Only Users and Groups with No Access permissions appear in the list.

Filter		Description
Mount USB	All	All Users and Groups appear in the list.
	Full Access	Only Users and Groups with Full Access Mount USB permissions appear in the list.
	Read Only	Only Users and Groups with Read Only Mount USB permissions appear in the list.
	No Access	Only Users and Groups with No Access Mount USB permissions appear in the list.
Config	All	All Users and Groups appear in the list.
	Permitted	Only Users and Groups with Permitted Config permissions appear in the list.
	Restricted	Only Users and Groups with Restricted Config permissions appear in the list.
PON	All	All Users and Groups appear in the list.
	Permitted	Only Users and Groups with Permitted PON permissions appear in the list.
	Restricted	Only Users and Groups with Restricted PON permissions appear in the list.

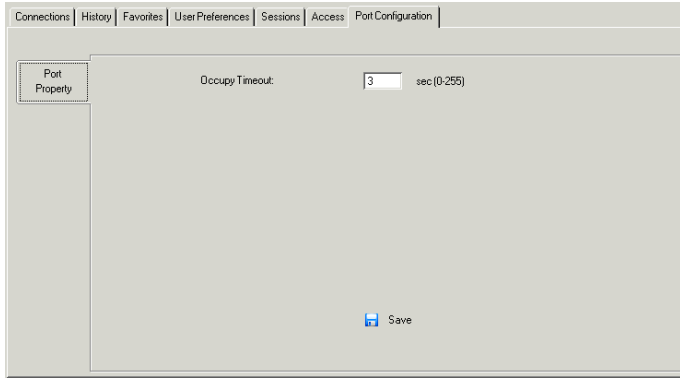
Saving Changes

Click the **Save** button at the lower right corner of the page to save any changes made on the Access page.

Port Configuration

Device Level

When a device is selected in the Sidebar, the only item available under Port Configuration is the Port Properties page with one field to configure: the *Occupy Timeout* setting:



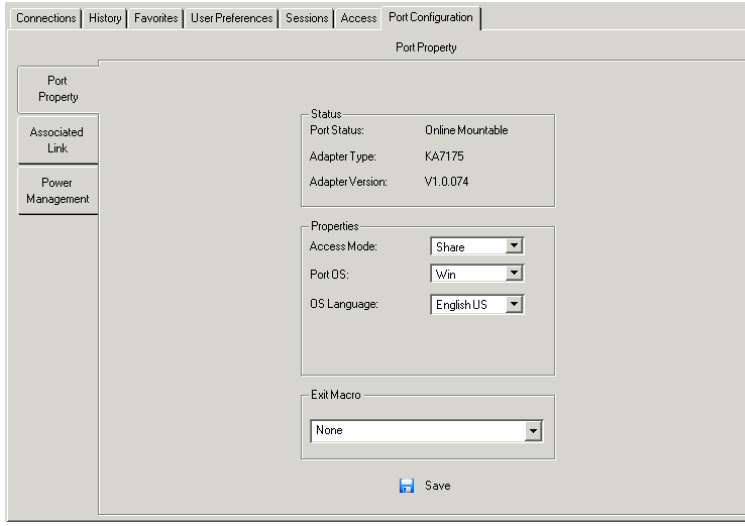
The Occupy Timeout field sets a time threshold for users on ports whose Access Mode has been set to Occupy (see *Access Mode*, page 128). If there is no activity from the user occupying the port for the amount of time set here, the user is timed out and the port is released. The first user to send keyboard or mouse input after the port has been released gets to occupy the port.

Input a value from 0 to 255 seconds. The default is 3 seconds. A setting of 0 causes the port to be released the instant there is no input.

Port Level

Port Properties

When a port is selected in the Sidebar, the Port Properties page looks similar to the one below:



- The *Status* panel provides information as to whether or not the port is online or offline; the Adapter cable used to connect the server (or other device) to the port; and the Adapter's firmware level.
- The *Properties* panel allows you to make configuration settings for the selected port. An explanation of the Port Properties configuration fields is given on the next page, please refer to the table on page 128 for further details.
- The *Exit Macro* panel contains a dropdown listbox of user created System macros. You can select a macro from the list that will execute when exiting the remote server. See *System Macros*, page 70 for details on creating exit macros.

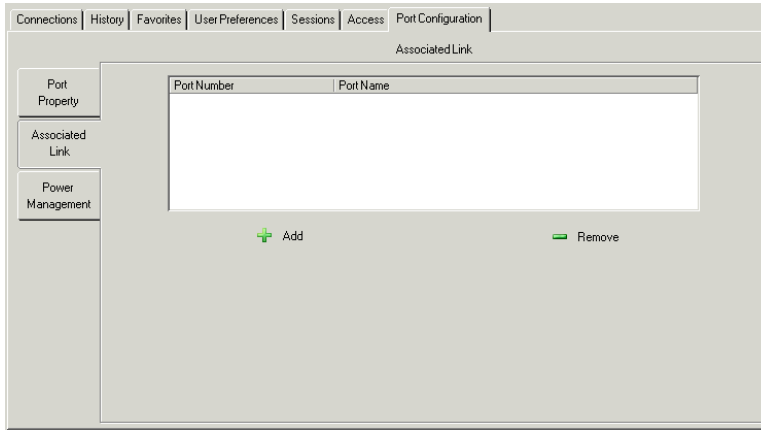
An explanation of the configuration fields is given in the table, below:

Field	Explanation
Port OS	Specifies the operating system that the server on the connected port is using. Choices are Win, Mac, Sun, and Other. The default is Win.
OS Language	Specifies the OS language being used by the server on the connected port. Drop down the list to see the available choices. The default is English US.
Access Mode	Defines how the port is to be accessed when multiple users have logged on, as follows: **Exclusive:** The first user to switch to the port has exclusive control over the port. No other users can view the port. The *Timeout* function does not apply to ports which have this setting. **Occupy:** The first user to switch to the port has control over the port. However, additional users may view the port's video display. If the user who controls the port is inactive for longer than the time set in the *Timeout* box, port control is transferred to the first user to move the mouse or strike the keyboard. **Share:** Users simultaneously share control over the port. Input from the users is placed in a queue and executed chronologically. Under these circumstances, users can take advantage of the *Message Board*, which allows users to communicate with each other regarding control of the keyboard and mouse or keyboard, mouse, and video of a Share port (see *The Message Board*, page 78).

When you have finished making your configuration changes, click **Save.**

Associated Links

The Associated Links page provides a method of associating other ports on the same switch to the selected port. This function is primarily intended to be used when connecting both KVM and serial ports (KA7140, KA9140) from a single server to the switch.

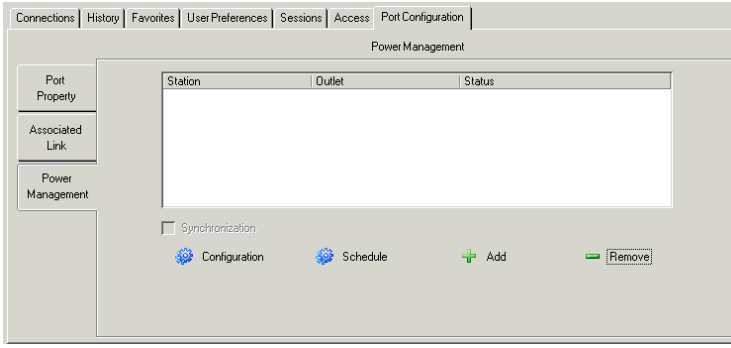


- To associate a port with the currently selected one, click **Add**. In the dialog box that appears, key in the port's number, then click **OK**. The port's number and name appear in the main panel.
- To remove an unwanted associated port, select it in the main panel, then click **Remove**.

Power Management

The *Power Management* page is used to associate a PON power outlet with a KVM port on the KVM over IP switch. Once an association has been made, the power status of the device attached to the KVM port can be controlled from the Port Access page, rather than having to control the power status by opening a separate web session to the PON device.

When the Power Management page comes up, it looks similar to the one below:



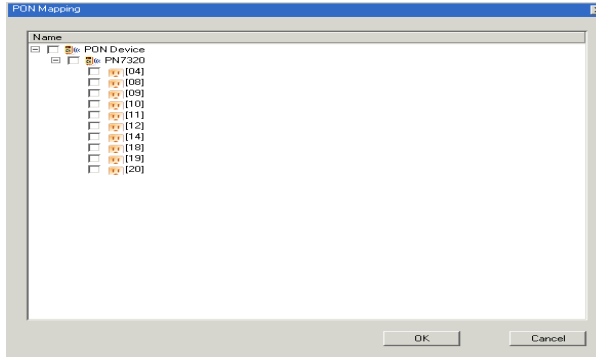
Note: This page is only available when a PON device is connected to the switch.

- Adding/Removing Associations:

  To associate an outlet with the selected port, do the following:

  1. Click **Add**.

     The PON Mapping dialog box comes up with a list of all the outlets available for association.

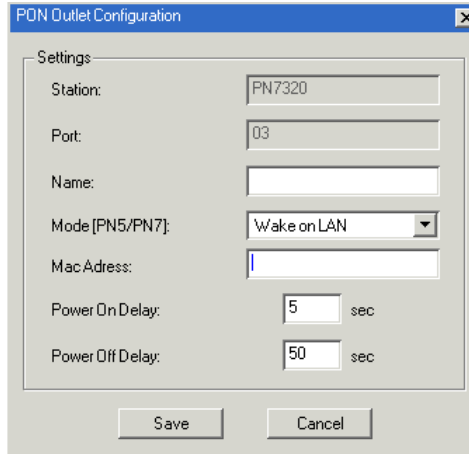


2. Check the outlet or outlets you want to associate with the port.
3. Click **OK**.

To disassociate an outlet from a port, select it in the main panel and click **Remove**.

- Configuration

You can configure an outlet's settings directly from this page by clicking the *Configuration* button. When you do, the *Pon Outlet Configuration* dialog box appears:



Set the configuration options according to the information in the table, below:

Heading	Explanation
Station	The name of the device that the outlet belongs to.
Port	The outlet's current name
Name	An editable field for naming the outlet. Each outlet can be given a distinctive name. The maximum number of characters is 15.

Heading	Explanation
Mode	Drop down the list to select a choice of power operation mode, as follows: ◆ *Wake On LAN*, and *System after AC Back* are Safe Shutdown and Reboot options, and can be used for scheduled restarts. When an Outlet's Power Button is clicked OFF, the PON device first sends a message to the computer telling it to prepare for a shutdown; it then waits for the amount time set in the *Power Off Delay* field to give the computer time to close down, and then turns off the power. When it is time to turn the power On, the PON device waits for the amount time set in the *Power On Delay* field, and then - depending on the mode chosen - either calls the computer's modem or sends an Ethernet message to the computer instructing it to start up again. **Note:** Refer to your PON manual for details on setting up Safe Shutdown and Reboot. ◆ If *Kill the Power* is selected, the PON device waits for the amount time set in the Power Off Delay field, and then turns the Outlet's power Off. Turning the power off performs a cold (non-safe) shutdown. There is no scheduled restart available with this shutdown method.
Mac Address	The Mac Address of the PON unit goes here.
Power On Delay	Sets the amount of time the PON device waits after the Power Button is clicked before it turns on the computer attached to the corresponding outlet. **Note:** The default delay time is 0 seconds; the maximum is 999 seconds. When a series of outlets are scheduled to be powered up, they turn on in sequence with a default delay of 10 milliseconds between each outlet.
Power Off Delay	Sets the amount of time the PON device waits after the Power Button is clicked before it shuts down the computer attached to the corresponding outlet. For the *System after AC Back* option, after the delay time expires, the PON device waits another fifteen seconds, then shuts the computer down. The default delay time is 15 seconds. The maximum delay time is 999 seconds.

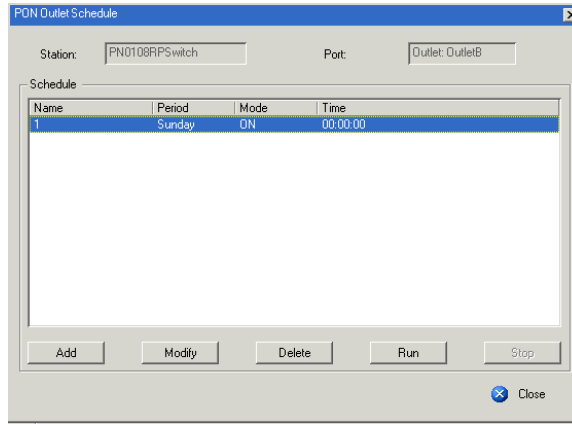
- Schedule

  Clicking the *Schedule* button brings up a dialog box that lets you set up an automated power management configuration for the outlet(s) associated with the selected port.

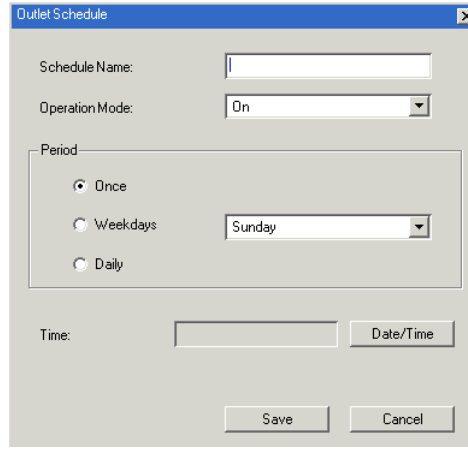
  - Adding an Outlet Schedule

    To set up an outlet schedule, do the following:

    1. Select the desired outlet in the main panel, then click **Schedule**. The *PON Outlet Schedule* dialog box with default settings, similar to the one below, comes up:



    2. Click **Add**. An *Outlet Schedule* dialog box, similar to the one below, comes up:



3. Configure the outlet according to the information provided in the following table:

Field	Explanation
Schedule Name	Provide a name to identify the scheduled operation by.
Operation Mode	Select the type of power operation you want to occur at the scheduled time.
Period	Select the time period that the scheduled operation will occur at: Once; Weekdays; or Daily – then drop down the list to select which day the operation is to start on.
Time	Click the *Date/Time* button to select the time and date the operation is to start on.

Note: If there is a conflict between the day set in the Period panel and the time the operation is supposed to start, a message will appear informing you of the problem. Click the *Date/Time* button and reset the time and date.

4. When you have finished making your configuration settings, click **Save**.

5. Repeat the above steps to set up additional schedules.

- To modify a schedule, select it in the main panel, then click **Modify**. The *Outlet Schedule* dialog box comes up – make your changes, then click **Save**.
- To delete a schedule, select it in the main panel, then click **Remove**.
- To run all power operations listed in the *Outlet Schedule* dialog box now – without waiting for the scheduled time to arrive – click **Run**.
- To stop all power operations listed in the *Outlet Schedule* dialog box, click **Stop**.
- Synchronization

  If more than one outlet has been selected for association with a port, *Synchronization* can be used to standardize their configurations.

  Enabling *Synchronization* (by checking the checkbox), brings up the *Pon Outlet Configuration* dialog box (see *Configuration*, page 131).

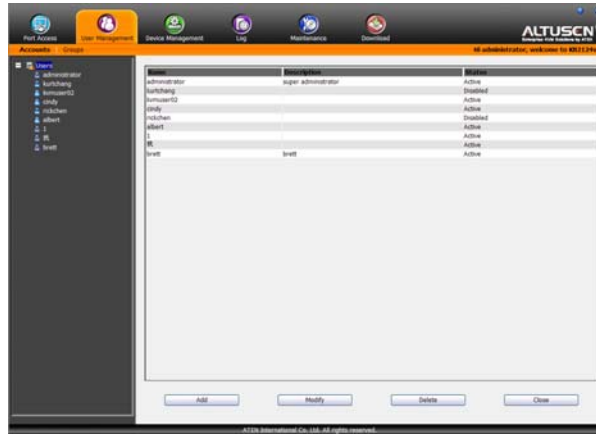
  The settings that you make are applied to all the outlets associated with the port so that their settings are all the same, and all the outlets associated with the port have the same schedule configuration as the first PON outlet.

Chapter 7
User Management

Overview

When you select the *User Management* tab the screen comes up with the *Users* page displayed:

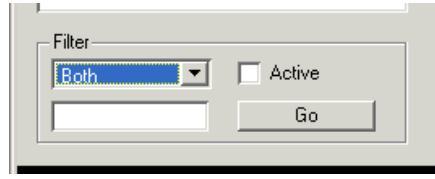
Browser GUI



AP GUI

The page is organized into two main areas: the Sidebar at the left, and the large main panel at the right.

- Users and groups appear in the panel at the left of the page. The large panel at the right provides more detailed information at-a-glance for each.
  - The Browser GUI has separate menu bar entries for Accounts (Users) and Groups. Depending on the menu item selected, either Users or Groups are listed in the Sidebar.
  - The AP GUI doesn't have menu entries. Instead, Users and Groups are listed separately in the Sidebar
- In the Browser GUI, the sort order of the information displayed can be changed by clicking the main panel column headings.
- In the AP GUI, the section below the Sidebar list provides a filter that allows you to manage the list:



  - Click the arrow at the right of the list box to select whether you want to view only Users, only, Groups, or both Users and Groups.
  - Click to put a check in the *Active* checkbox to filter out any users whose accounts are not active.
  - To only select Users or Groups that match a particular string, key it into the text box in front of the *Go* button, then click **Go**. Only Users or Groups that match the string will appear in the list.

    Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
- The buttons below the main panel are used to manage users and groups, as shown in the sections that follow.

Users

The KVM over IP switch supports three types of user, as shown in the table, bellow:

User Type	Role
Super Administrator	Access and manage ports and devices. Manage Users, and Groups. Configure the overall installation. Configure personal working environment.
Administrator	Access and manage authorized ports and devices. Manage Users and Groups. Configure personal working environment.
User	Access authorized ports and devices. Manage authorized ports and devices; configure personal working environment. **Note:** Users who have been given permission to do so, may also manage other users.

Adding Users

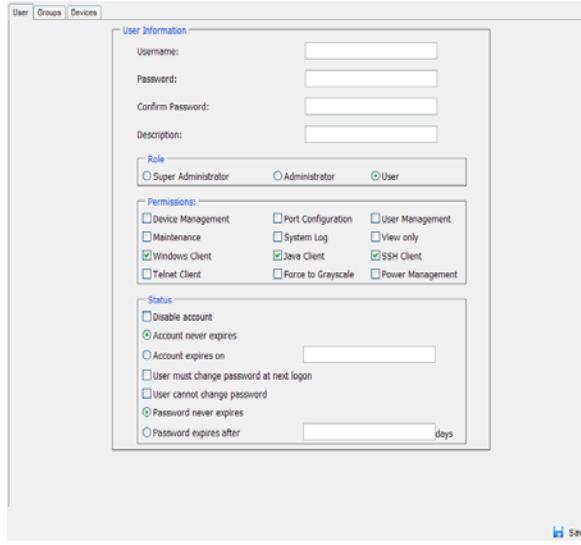
To add a user, and assign user permissions, do the following:

1. Select *Users* on the menu bar (Browser GUI)

   – or –

   Select *Users* in the Sidebar (AP GUI).

2. Click **Add** at the bottom of the main panel. The User notebook opens, with the *User* tab selected:



3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Username	From 1 to16 characters are allowed depending on the Account Policy settings. See *Account Policy*, page 178.
Password	From 0 to16 characters are allowed depending on the Account Policy settings. See *Account Policy*, page 178.
Confirm Password	To be sure there is no mistake in the password, you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.
Role	There are three categories: Super Administrator, Administrator and User. There is no limitation on the number of accounts that can be created in each category. ◆ The Super Administrator is responsible for the overall installation configuration and maintenance; user management; and device and port assignments. The Super Administrator's permissions (see page 139) are automatically assigned by the system and cannot be altered. ◆ The default permissions for Administrators include everything except *Force to Grayscale*, but the permissions can be altered for each Administrator by checking or unchecking any of the permissions checkboxes. ◆ The default permissions for Users include the Win, Java, and SSH clients, but the permissions can be altered for each User by checking or unchecking any of the permissions checkboxes. **Note:** Users who have been given User Management privileges cannot access or configure Groups.

Field	Description
Permissions **Note:** For ordinary users, in addition to enabling *Device Management*, *Port Configuration*, and *Maintenance* permissions, the user must also be given those rights for each device and port that he will be allowed to manage. See *Device Assignment*, page 149 for details.	◆ Enabling *Device Management* allows a user to configure and control the settings for overall KVM over IP switch operations (see *Device Management*, page 153). ◆ Enabling *Port Configuration* allows a user to configure and control the settings for individual ports (see *Port Configuration*, page 126). ◆ Enabling *User Management* allows a user to create, modify, and delete user and group accounts. ◆ Enabling *Maintenance* allows a user to perform all the Maintenance operations available under the Maintenance tab (see *Maintenance*, page 195). ◆ Enabling *System Log* allows a user to access the system log (see *Log*, page 191). ◆ Enabling *View Only* limits users to only being able to view the display of connected devices. They cannot control port access, nor can they input any keyboard or mouse signals to the devices they view. ◆ Enabling *Windows Client* allows a user to download the Windows Client AP software, and access the KVM over IP switch with it, in addition to (or instead of) the browser access method. ◆ Enabling *Java Client* allows a user to download the Java Client AP software, and access the KVM over IP switch with it, in addition to (or instead of) the browser access method. ◆ Enabling *SSH Client* allows a user to log in and access the KVM over IP switch via an SSH session. ◆ Enabling *Telnet Client* allows a user to log in and access the KVM over IP switch via a Telnet session. ◆ *Force to Grayscale* forces the user's view of the remote display to be in grayscale. This can speed up I/O transfer in low bandwidth situations.

Field	Description
Status	Status allows you to control the user's account and access to the installation, as follows: ◆ *Disable Account* lets you suspend a user's account without actually deleting it, so that it can be easily reinstated in the future. ◆ If you don't want to limit the time scope of the account, select *Account never expires*; if you do want to limit the amount of time that the account remains in effect, select *Account expires on*, and key in the expiration date. ◆ To require a user to change his password at the next logon, select *User must change password at next logon*. This can be used by the administrator to give the user a temporary password to log in for the first time, and then let the user set the password of his choice for future logins. ◆ To make a password permanent, so that the user cannot change it to something else, select *User cannot change password*. ◆ For security purposes, administrators may want users to change their passwords from time to time. ◆ If not, select *Password never expires*. This allows users to keep their current passwords for as long as they like. ◆ If so, select *Password expires after*, and key in the number of days allowed before the password expires. Once the time is up, a new password must be set.

4. At this point you can assign the new user to a group by selecting the *Groups* tab – the Groups page is discussed on page 145. You can also assign the user's port access rights by selecting the *Devices* tab – the Devices page is discussed on page 149.

Note: Optionally, you can skip this step now to add more users and create groups, and come back to it later.

5. When your selections have been made click **Save**.
6. When the *Operation Succeeded* message appears, click **OK**.

7. Click **Users** in the Sidebar to return to the main screen. The new user appears in the Sidebar list and in the main panel, as well.
   - The Sidebar *Users* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the *Users* icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
   - The icon for super administrators has two black bands; the icon for administrators has one red band.
   - The large main panel shows the user's name; the description that was given when the account was created; and whether the account is currently active or has been disabled.

Modifying User Accounts

To modify a user account, do the following:

1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name
2. Click **Modify**.
3. In the *User* page that comes up, make your changes, then click **Save**.

Note: The *User* page is discussed on page 137; the *Groups* page is discussed on page 145, the *Devices* page is discussed on page 149.

Deleting User Accounts

To delete a user account do the following:

1. In the main panel, select the user's name.
2. Click **Delete**.
3. Click **OK**.

Groups

Groups allow administrators to easily and efficiently manage users and devices. Since device access rights apply to anyone who is a member of the group, administrators need only set them once for the group, instead of having to set them for each user individually. Multiple groups can be defined to allow some users access to specific devices, while restricting other users from accessing them.

Creating Groups

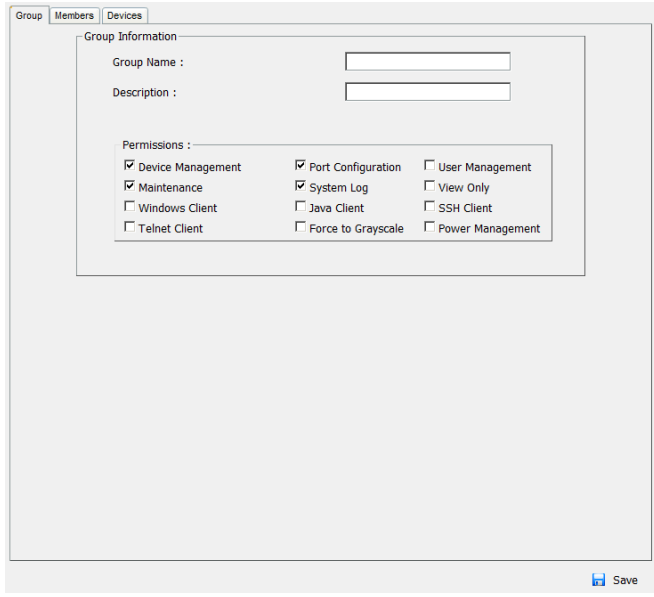
To create a group, do the following:

1. Select *Groups* on the menu bar (Browser GUI)

   – or –

   Select *Groups* in the Sidebar (AP GUI).

2. Click **Add** at the bottom of the main panel. The Group notebook opens, with the *Group* tab selected:



3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Group Name	A maximum of 16 characters is allowed.
Description	Additional information about the user that you may wish to include. A maximum of 63 characters is allowed.
Permissions	Permissions and restrictions for groups are set by checking the appropriate boxes. These are the same permissions as the ones specified for Users. See *Permissions*, page 139 for details

4. At this point you can assign users to the group by selecting the *Members* tab – the Members page is discussed on page 147. You can also assign the group's port access rights by selecting the *Devices* tab – the Devices page is discussed on page 149.

Note: Optionally, you can skip this step now to add more groups and assign users to them, and come back to it later.

5. When your selections have been made click **Save**.
6. When the *Operation Succeeded* message appears, click **OK**.
7. Click **Group** in the Sidebar to return to the main screen. The new group appears in the Sidebar Group list and in the main panel.
   - The Sidebar *Group* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the *Users* icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
   - The large main panel shows the group's name, and the description that was given when the group was created (the *Status* column is inactive).

Repeat the above procedure to add additional groups.

Note: You must perform Step 7 before attempting to add a new group, or else the new group you are creating will replace the group you just finished creating.

Modifying Groups

To modify a group, do the following:

1. In the Sidebar *Group* list, click the group's name
   – or –
   In the main panel, select the group's name.
2. Click **Modify**.
3. In the *Group* notebook that comes up, make your changes, then click **Save**.

Note: The *Group* page is discussed on page 142; the *Members* page is discussed on page 147, The *Devices* page is discussed on page 149.

Deleting Groups

To delete a group do the following:

1. In the Sidebar, click the *Groups* icon.
2. In the main panel, select the group's name.
3. Click **Delete**.
4. Click **OK**.

Users and Groups

There are two ways to manage users and groups: from the Users notebook; and from the Group notebook.

Note: Before you can assign users to groups, you must first create them. See *Adding Users*, page 137 for details.

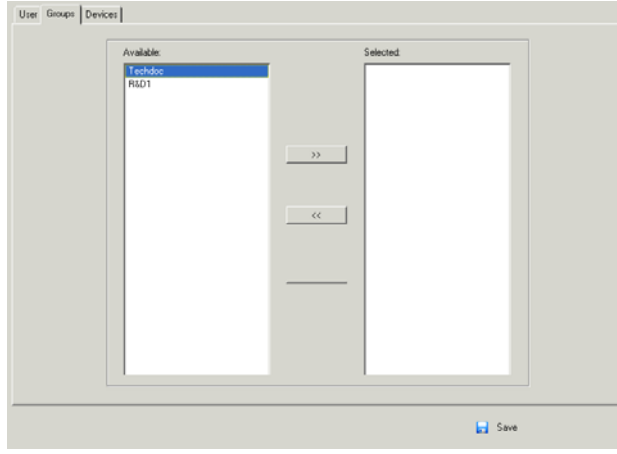
Assigning Users to a Group From the User's Notebook

To assign a user to a group from the User's notebook, do the following:

1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name
2. Click **Modify**.
3. In the *User* notebook that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the group that you want the user to be in.
5. Click the **Right Arrow** to put the group's name into the *Selected* column.
6. Repeat the above for any other groups that you want the user to be in.
7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the User's Notebook

To remove a user from a group from the User's notebook, do the following:

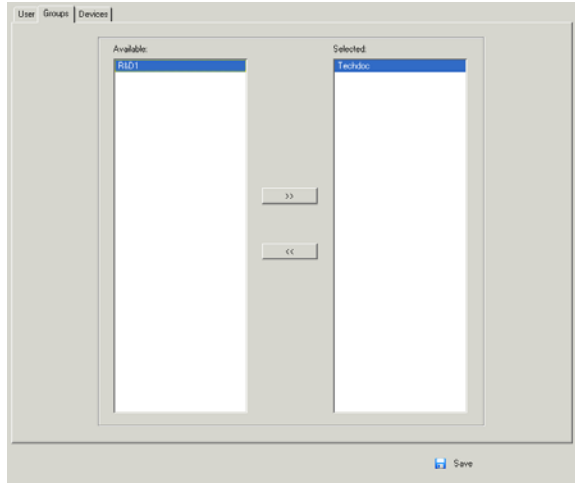
1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the group that you want to remove the user from.

5. Click the **Left Arrow** to remove the group's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other groups that you want to remove the user from.

7. Click **Save** when you are done.

Assigning Users to a Group From the Group's Notebook

To assign a user to a group from the Group notebook, do the following:

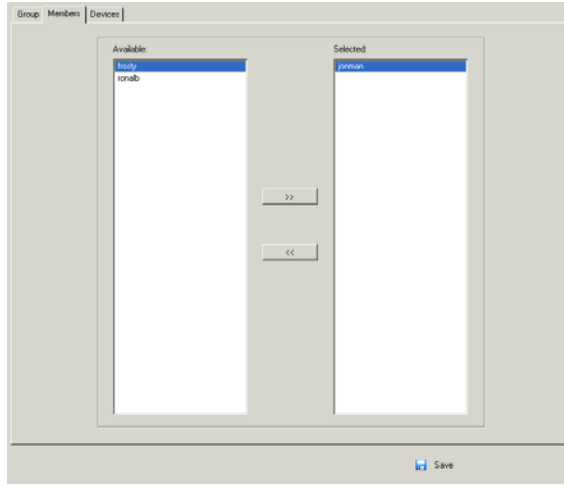
1. In the Sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the user that you want to be a member of the group.

5. Click the **Right Arrow** to put the user's name into the *Selected* column.

6. Repeat the above for any other users that you want to be members of the group.

7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the Group's Notebook

To remove a user from a group from the Group's notebook, do the following:

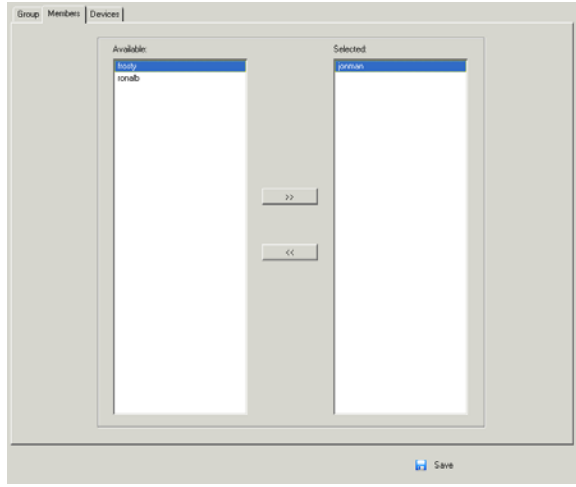
1. In the Sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the user that you want to remove from the group.

5. Click the **Left Arrow** to remove the user's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other users that you want to remove from the group.

7. Click **Save** when you are done.

Device Assignment

When a user logs in to the KVM over IP switch, the interface comes up with the Port Access page displayed. All the ports that the user is permitted to access are listed in the Sidebar at the left of the page. Access permissions for those ports and the devices connected to them are assigned on a port-by-port basis from the *User* or *Group* list on the Sidebar of the User Management page.

Assigning Device Permissions From the User's Notebook

To assign a device permissions to a user from the *User's* notebook, do the following:

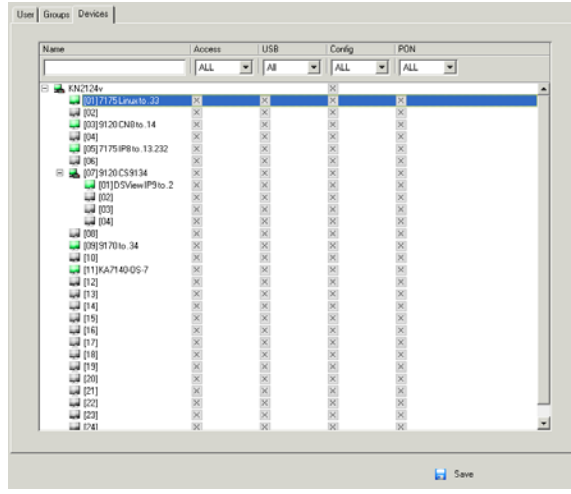
1. In the Sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Devices* tab. A screen, similar to the one below, appears:



4. Make your permission settings for each port according to the information provided below:

Name: Each port accessible to the user is listed under the *Names* column.

Access: The *Access* column is where device access rights are set. Click the icon in the row that corresponds to the port you want to configure to cycle through the choices. The meanings of the icons are described in the table, below:

	Full Access	The user can view the remote screen and can perform operations on the remote server from his keyboard and monitor.
	View Only	The user can only view the remote screen; he cannot perform any operations on it.
	No Access	No access rights - the Port will not show up on the User's list on the Main Screen.

USB: The *USB* column is where USB Virtual Media device access rights are listed. This entry does not appear for switches that do not support the USB Virtual Media function. Click the icon in the row that corresponds to the port you want to configure to cycle through the choices.

Full Access means that the User can mount, read, and write the virtual media; *View Only* means that the user can only read already mounted virtual media data.

Config: The *Config* column is where a user's permission to make changes to a port's configuration settings are permitted/ restricted. Click the icon in the row that corresponds to the port you want to configure to cycle through the choices.

A check mark (√) indicates that the user has permission to make changes to the port's configuration settings; an X means that the user is denied permission to make configuration changes.

PON: The PON column permits/restricts the configuration and power operation of ports that have Power Over the Net™ devices connected to them. A check mark (√) indicates that the user has permission; an X means that the user does not have permission.

5. When you have finished making your choices, click **Save**.
6. In the confirmation popup that appears, click **OK**.

Note: In any of the columns, you can use Shift-Click or Ctrl-Click to select a group of ports to configure. Clicking to cycle through the choices on any one of the selected ports causes all of them to cycle in unison.

Filters

There are five filters at the top of the columns that allow you to expand or limit the scope of the ports that are displayed in the *Name* column, as described in the following table:

Filter		Description
Name		To filter on the port name, key in the name then press **Enter**. Only the ports whose names correspond to what you have keyed in appear in the list. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
Access	All	All ports appear in the list.
	Full Access	Only ports configured as Full Access ports appear in the list.
	View Only	Only ports configured as View Only ports appear in the list.
	No Access	Only ports configured as No Access ports appear in the list.
USB	All	All ports appear in the list.
	Full Access	Only ports configured as Full Access USB ports appear in the list.
	Read Only	Only ports configured as Read Only USB ports appear in the list.
	No Access	Only ports configured as No Access USB ports appear in the list.
Config	All	All ports appear in the list.
	Permitted	Only ports configured as Permitted appear in the list.
	Restricted	Only ports configured as Restricted appear in the list.
PON	All	All ports appear in the list.
	Permitted	Only ports configured as Permitted appear in the list.
	Restricted	Only ports configured as Restricted appear in the list.

Assigning Device Permissions From the Groups' Notebook

To assign a device permissions to a Group of users, do the following:

1. In the Sidebar *Groups* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Groups* notebook that comes up, select the *Devices* tab.

4. The screen that comes up is the same one that appears in the User's notebook. The only difference is that whatever settings you make apply to all members of the group instead of just one individual member.

   Make your device assignments according to the information described under *Assigning Device Permissions From the User's Notebook*, page 149.

Chapter 8
Device Management

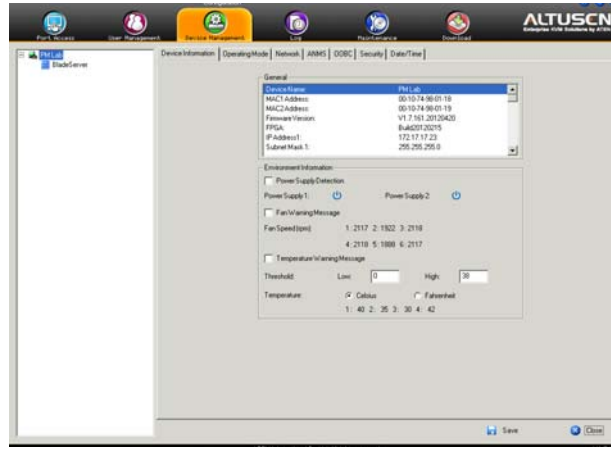
KVM Devices

Device Information

The Device Management page opens with the top level KVM over IP switch selected in the Sidebar and the *Device Information* item selected on the menu bar:

Browser GUI

AP GUI



General

The *General* section of the Device Information page displays the name of the selected device, its firmware version, the FPGA (Field-Programmable-Gate-Array) and information about its network configuration.

Note: The AP GUI version presents the same information as the Browser version. Scroll through the list to see the additional entries.

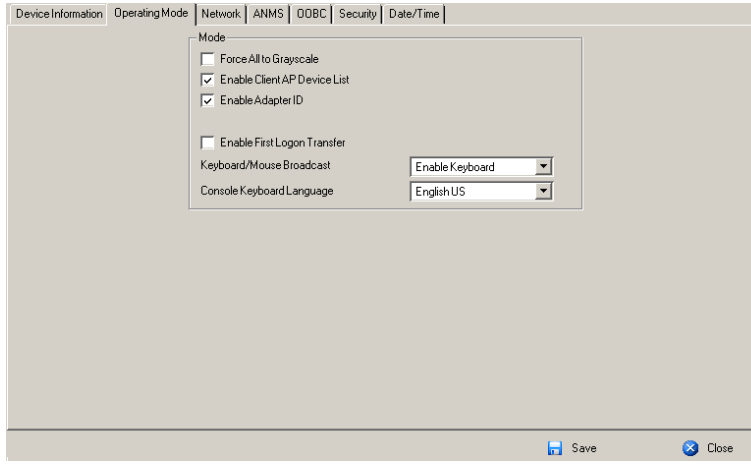
Environment

The lower panel presents information concerning the device's environment, as described in the table, below:

Item	Description
Power Supply Detection	The icons for Power Supply 1 and Power Supply 2 display in gray when there is no power to the power supply – they display in blue when power is present. When this function is enabled (there is a check in the checkbox), if there is only one source of power, the switch will beep constantly to warn you of the problem. If you are at the Local Console you will see a message asking you to confirm that your intention is to only have one power source. If your intention is to only have one source of power, there are two ways to stop the beeping: 1) You can disable power supply warnings by unchecking the checkbox. Do this if you want to disable this function on a permanent basis. Or, 2) you can confirm your intention in the dialog box. Do this if you only want to disable the warning temporarily. With this method, the warning function will be back in effect after the next system reset. The default for this function is enabled.
Fan Warning Message	Place a check in the checkbox to enable a fan warning message. If this function is enabled, when any fan stops spinning the system records the event in the system log. If it is not enabled, the event will not be recorded. **Note:** The warning doesn't necessarily mean that the fan has failed, since the fan will stop spinning (as desired) when the temperature drops below its lower setting. The default for this function is enabled.
Fan Speed	Fan speeds are indicated here. See *Fan Location and Speed Information*, page 273.

Item	Description
Temperature Warning Message	Place a check in the checkbox to enable a temperature warning message. If this function is enabled, when the device's temperature drops below the Low threshold setting, or exceeds the High threshold setting, the system records the event in the system log. If it is not enabled, the event will not be recorded. The default for this function is enabled.
Temperature	Temperature readings from the switch's built-in sensors are indicated here and can be displayed in degrees Celsius or Fahrenheit. See *Clear Login Information*, page 274

Operating Mode



The Operating Mode page is used to set working parameters, as described below:

- If *Force all to grayscale* is enabled, the remote displays of all devices connected to the KVM over IP switch are changed to grayscale. This can speed up I/O transfer in low bandwidth situations.
- If *Enable Client AP Device List* is enabled, the switch appears in the Server List when using the WinClient or Java Client AP (see *Windows Client AP Login*, page 45, and *Java Client AP Login*, page 49). If this option is not enabled, the switch can still be connected to, but its name will not appear in the Server List.

- When the *Enable Adapter ID* function is enabled (the default) the switch stores adapter cable information for each of its ports, so that when you move a KVM Adapter Cable from one port to another, it remembers the adapter cable's port properties information at the new location (see *The Adapter ID Function*, page 34).
- If *Enable First Logon Transfer* is enabled, only the first user on a bus can switch ports. Other users on the bus cannot switch ports unless there is a bus that is already connected to the port they would like to access, or there is a free bus available. (For details regarding users and buses, see *Users and Buses*, page 219.)
- For the *Keyboard/Mouse Broadcast* setting, drop down the list to make your choice.
  - If you enable Keyboard Broadcast, your keystrokes will be duplicated on all the attached servers that currently appear in the Sidebar.
  - If you enable Mouse Broadcast, your mouse movements and clicks will be duplicated on all the attached servers that currently appear in the Sidebar.

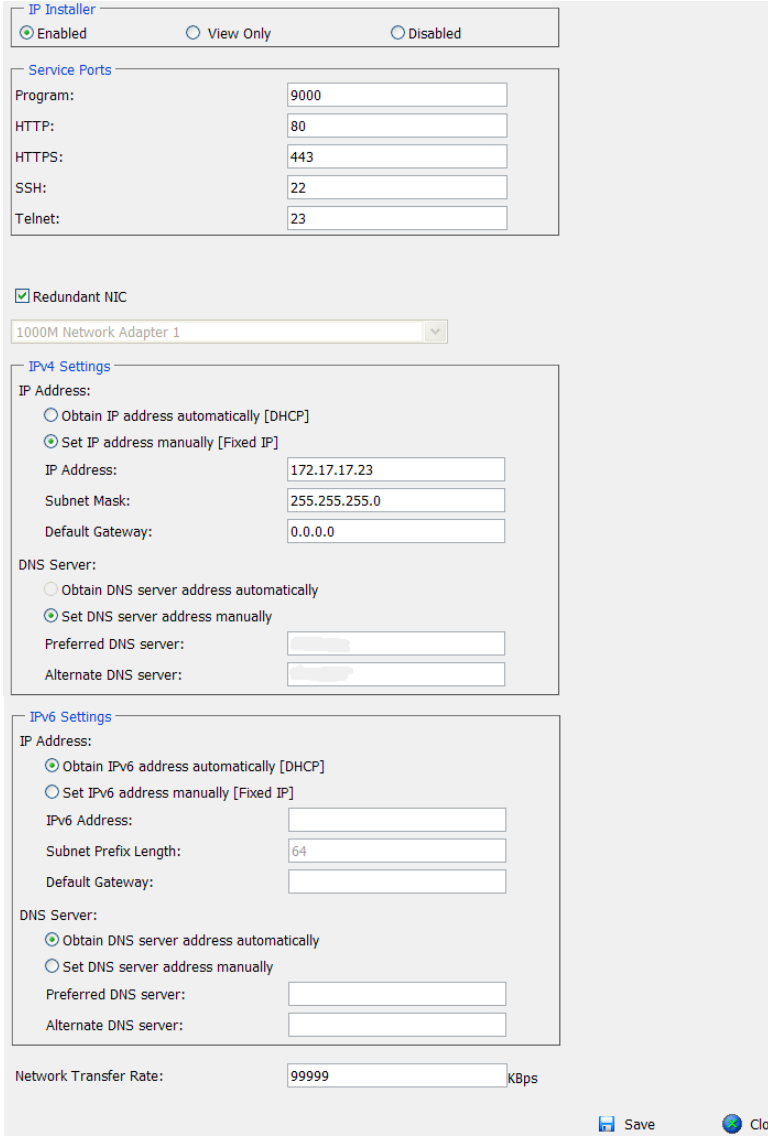
  Note: 1. On a KVM switch that is cascaded from the KVM over IP switch, only one port can perform a Keyboard/Mouse broadcast at a time.

  2. For Mouse Broadcast, you and all the servers must be running the same OS; all the monitors must have the same resolution; and all the screens must have an identical layout.

- The *Console Keyboard Language* setting lets you specify which keyboard mapping is being used by the Local Console keyboard. Drop down the list to make your choice.

Network

The Network page is used to specify the network environment.



Each of the elements on this page is described in the sections that follow.

IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the KVM over IP switch.

Click one of the radio buttons to select *Enable*, *View Only*, or *Disable* for the IP Installer utility. See *IP Installer*, page 250, for IP Installer details.

Note: 1. If you select *View Only*, you will be able to see the KVM over IP switch in the IP Installer's Device List, but you will not be able to change the IP address.

2. For security, we strongly recommend that you set this to *View Only* or *Disable* after each use.

Service Ports

As a security measure, if a firewall is being used, the Administrator can specify the port numbers that the firewall will allow. If a port other than the default is used, users must specify the port number as part of the IP address when they log in. If an invalid port number (or no port number) is specified, the KVM over IP switch will not be found. An explanation of the fields is given in the table below:

Field	Explanation
Program	This is the port number for connecting with the WinClient ActiveX Viewer, WinClient AP, Java Client Viewer, Java Client AP, or via Virtual Media. The default is 9000.
HTTP	The port number for a browser login. The default is 80.
HTTPS	The port number for a secure browser login. The default is 443.
SSH	The port for SSH access. The default is 22.
Telnet	The port for Telnet access. The default is 23.

Note: 1. Valid entries for all of the Service Ports are from 1–65535.

2. Service ports cannot have the same value. You must set a different value for each one.

3. If there is no firewall (on an Intranet, for example), it doesn't matter what these numbers are set to, since they have no effect.

NIC Settings

- Redundant NIC

  The KVM over IP switch is designed with two network interfaces. If *Redundant NIC* is enabled (the default), both interfaces make use of the IP address of Network Adapter 1.

  Under this configuration, the second interface is usually inactive. If there is a network failure on the first interface, the switch automatically switches to the second interface.

  - Redundant NIC Enabled – Single IP Address for Both Interfaces

    To enable the Redundant NIC function, do the following:

    1. Click to put a check in the *Redundant NIC* checkbox.
    2. *Network Adapter 1* is selected in the network adapter listbox, and the listbox is disabled – you cannot configure Network Adapter 2.
    3. Configure the IP and DNS server addresses for Network Adapter 1 (see the sections below).

  - Redundant NIC Not Enabled – Two IP Addresses

    If you choose not to enable the Redundant NIC function, the two NICs can be configured with separate interfaces. Users can log into the KVM over IP switch with either IP address. To set up the switch with this configuration, do the following:

    1. If there is a check in the *Redundant NIC* checkbox, click to remove it.
    2. In the network adapter listbox; select Network Adapter 1.
    3. Configure the IP and DNS server addresses for Network Adapter 1 (see the sections below).
    4. Drop down the network adapter listbox; select Network Adapter 2.
    5. Configure the IP and DNS server addresses for Network Adapter 2.

- IPv4 Settings
  - IP Address:

    IPv4 is the traditional method of specifying IP addresses. The KVM over IP switch can either have its IP address assigned dynamically (DHCP), or it can be given a fixed IP address.

    - For dynamic IP address assignment, select the *Obtain IP address automatically* radio button. (This is the default setting.)
    - To specify a fixed IP address, select the *Set IP address manually* radio button and fill in the fields with values appropriate for your network.

    Note: 1. If you choose *Obtain IP address automatically*, when the switch starts up it waits to get its IP address from the DHCP server. If it hasn't obtained the address after one minute, it automatically reverts to its factory default IP address (192.168.0.60.)

    2. If the switch is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see *IP Address Determination*, page 250, for information./

  - DNS Server
    - For automatic DNS Server address assignment, select the *Obtain DNS Server address automatically* radio button.
    - To specify the DNS Server address manually, select the *Set DNS server address manually* radio button, and fill in the addresses for the Preferred and Alternate DNS servers with values appropriate for your network.

    Note: Specifying the Alternate DNS Server address is optional.

- IPv6 Settings
  - IP Address:

    IPv6 is the new (128-bit) format for specifying IP addresses. (See *IPv6*, page 252 for further information.) The KVM over IP switch can either have its IPv6 address assigned dynamically (DHCP), or it can be given a fixed IP address.

    - For dynamic IP address assignment, select the *Obtain IP address automatically* radio button. (This is the default setting.)
    - To specify a fixed IP address, select the *Set IP address manually* radio button and fill in the fields with values appropriate for your network.
  - DNS Server
    - For automatic DNS Server address assignment, select the *Obtain DNS Server address automatically* radio button.
    - To specify the DNS Server address manually, select the *Set DNS server address manually* radio button, and fill in the addresses for the Preferred and Alternate DNS servers with values appropriate for your network.

    Note: Specifying the Alternate DNS Server address is optional.

Network Transfer Rate

This setting allows you to tailor the size of the data transfer stream to match network traffic conditions by setting the rate at which the KVM over IP switch transfers data between itself and the client computers. The range is from 4–99999 Kilobytes per second (KBps).

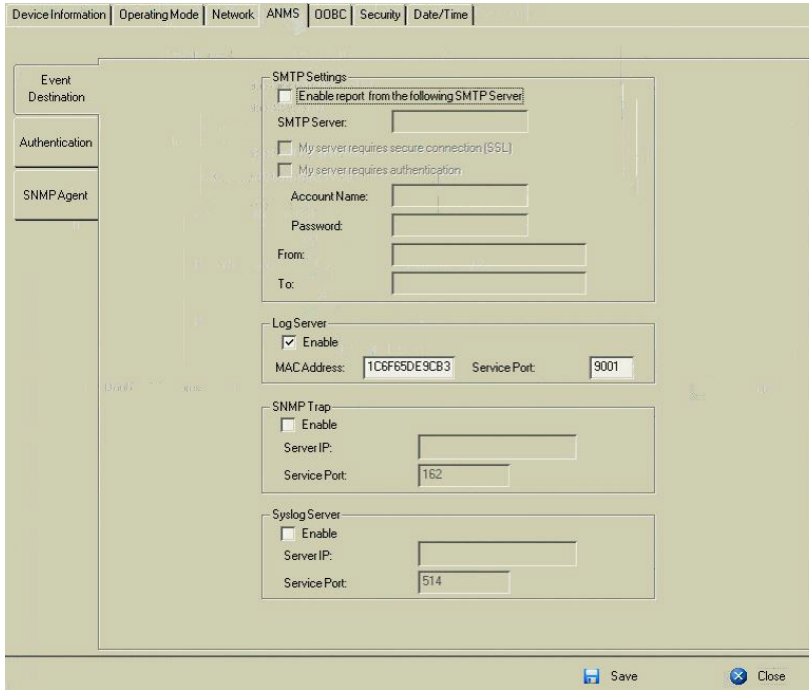
Finishing Up

After making any network changes, be sure *Reset on exit* on the *Device Management → System Operation* page (see *Reset on exit:*, page 206) has been enabled (there is a check in the checkbox), before logging out. This allows network changes to take effect without having to power the switch off and on.

ANMS

The ANMS (Advanced Network Management Settings) page is used to set up login authentication and authorization management from external sources. It is organized as a notebook with two tabs – each with a series of related panels, as described, below:

Event Destination



- SMTP Settings

  To have the KVM over IP switch email reports from the SMTP server to you, do the following:

  1. Enable the *Enable report from the following SMTP server*, and key in either the IPv4 address, IPv6 address, or domain name of the SMTP server.
  2. If your server requires a secure SSL connection, put a check in the *My server requires secure connection (SSL)* checkbox.

3. If your server requires authentication, put a check in the *My server requires authentication* checkbox, and key in the appropriate account information in the *Account Name* and *Password* fields.
4. Key in the email address of where the report is being sent from in the *From* field.

Note: 1. Only one email address is allowed in the *From* field, and it cannot exceed 64 Bytes.

2. 1 Byte = 1 English alphanumeric character.

5. Key in the email address (addresses) of where you want the SMTP reports sent to in the *To* field.

Note: If you are sending the report to more than one email address, separate the addresses with a semicolon. The total cannot exceed 256 Bytes.

- Log Server

  Important transactions that occur on the KVM over IP switch, such as logins and internal status messages, are kept in an automatically generated log file.

  - Specify the MAC address of the computer that the Log Server runs on in the *MAC address* field.
  - Specify the port used by the computer that the Log Server runs on to listen for log details in the *Port* field. The valid port range is 1–65535. The default port number is 9001.

  Note: The port number must different than the one used for the *Program* port (see *Program*, page 158).

  See Chapter 13, *The Log Server*, for details on setting up the log server. The Log File is discussed on page 191.

- SNMP Trap

  To be notified of SNMP trap events, do the following:

  1. Check *Enable SNMP Agent*.
  2. Key in either the IPv4 address, IPv6 address, or domain name of the computer to be notified of SNMP trap events.
  3. Key in the port number. The valid port range is 1–65535.

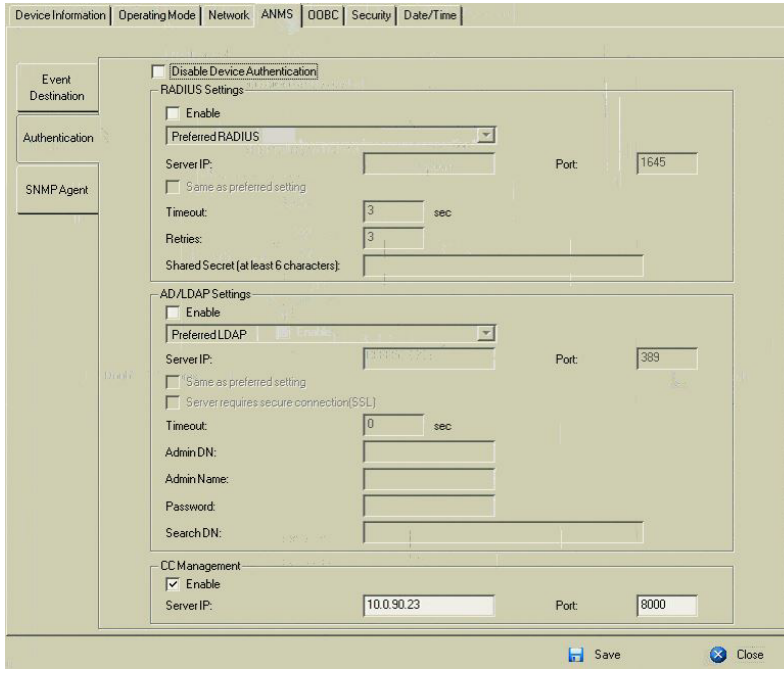
  Note: The logs that are notified of SNMP trap events are configured on the Notification Settings page under the Log tab. See *Log Notification Settings*, page 194 for details.

- Syslog Server

  To record all the events that take place on KVM over IP switches and write them to a Syslog server, do the following:

  1. Check **Enable**.
  2. Key in either the IPv4 address, IPv6 address, or domain name of the Syslog server.
  3. Key in the port number. The valid port range is 1-65535.

Authentication



- Disable Local Authentication

  Selecting this option disables login authentication on the KVM over IP switch. The switch can only be accessed using LDAP, LDAPS, MS Active Directory, RADIUS or CC Management authentication.

- RADIUS Settings

  To allow authentication and authorization for the KVM over IP switch through a RADIUS server, do the following:

  1. Check **Enable**.
  2. Select Preferred or Alternate RADIUS server.
  3. Fill in the IP addresses and service port numbers for the Preferred and Alternate RADIUS servers. You can use the IPv4 address, the IPv6 address or the domain name in the IP fields.
  4. In the *Timeout* field, set the time in seconds that the KVM over IP switch waits for a RADIUS server reply before it times out.
  5. In the *Retries* field, set the number of allowed RADIUS retries.

6. In the *Shared Secret* field, key in the character string that you want to use for authentication between the KVM over IP switch and the RADIUS Server. A minimum of 6 characters is required.
7. On the RADIUS server, Users can be authenticated with any of the following methods:
   - Set the entry for the user as **su/xxxx**

     Where *xxxx* represents the Username given to the user when the account was created on the KVM over IP switch.
   - Use the same Username on both the RADIUS server and the KVM over IP switch.
   - Use the same Group name on both the RADIUS server and the KVM over IP switch.
   - Use the same Username/Group name on both the RADIUS server and the KVM over IP switch.

   In each case, the user's access rights are the ones assigned that were assigned when the User of Group was created on the KVM over IP switch. (See *Adding Users*, page 137.)

- LDAP / LDAPS Authentication and Authorization Settings

  To allow authentication and authorization for the KVM over IP switch via LDAP / LDAPS, refer to the information in the table, below:

Item	Action
Enable	Put a check in the *Enable* checkbox to allow LDAP / LDAPS authentication and authorization.
Type	Click a radio button to specify whether to use LDAP or LDAPS.
LDAP Server IP and Port	Select Preferred or Alternate LDAP Server and fill in the IP address and port number for the LDAP or LDAPS server. ◆ You can use the IPv4 address, the IPv6 address or the domain name in the *LDAP Server* field. ◆ For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Admin DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: ou=kn8132,dc=aten,dc=com
Admin Name	Key in the LDAP administrator's username.
Password	Key in the LDAP administrator's password.

Item	Action
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names.
Timeout	Set the time in seconds that the KVM over IP switch waits for an LDAP or LDAPS server reply before it times out.

On the LDAP / LDAPS server, Users can be authenticated with any of the following methods:

- With MS Active Directory schema.
- Without schema – Only the Usernames used on the KVM over IP switch are matched to the names on the LDAP / LDAPS server. User privileges are the same as the ones configured on the switch.
- Without schema – Only Groups in AD are matched. User privileges are the ones configured for the groups he belongs to on the switch.
- Without schema – Usernames and Groups in AD are matched. User privileges are the ones configured for the User and the Groups he belongs to on the switch.

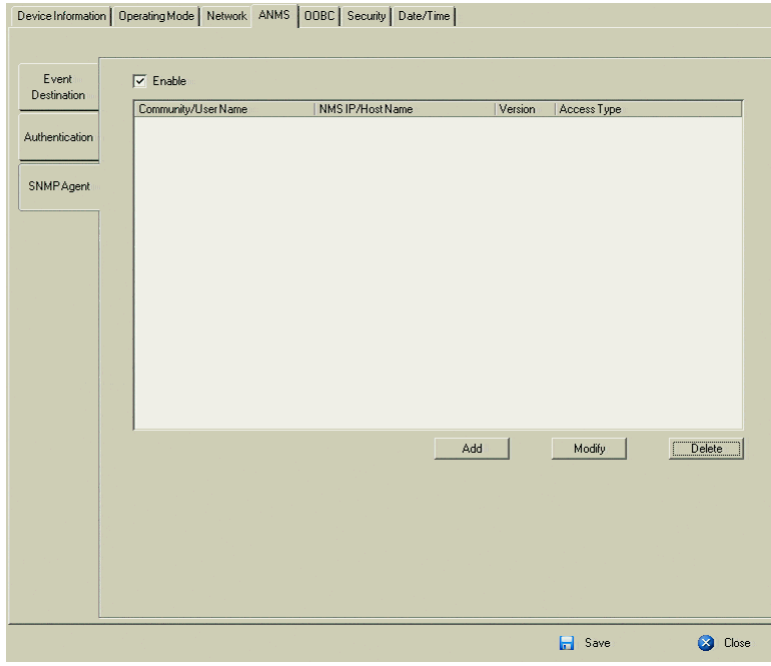
Note: For more information on configuring LDAP, you can download the full LDAP instructional manual from our website.

CC Management Settings

To allow authorization for the KVM over IP switch through a CC (Control Center) server, check *Enable* and fill in the CC Server's IP address and Service port in the appropriate fields. You can use the IPv4 address, the IPv6 address or the domain name in the *CC Server IP* field.

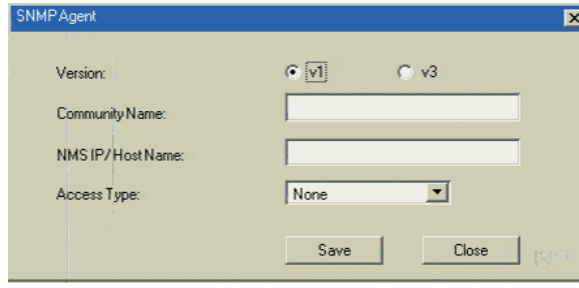
Note: If this function is enabled, PON devices do not appear in the Sidebar, even if they are configured on the switch. This is because they are managed via the CC server.

SNMP Agent



To set SNMP Agent, do the following:

1. Check **Enable**.
2. Click **Add**. A window appears:

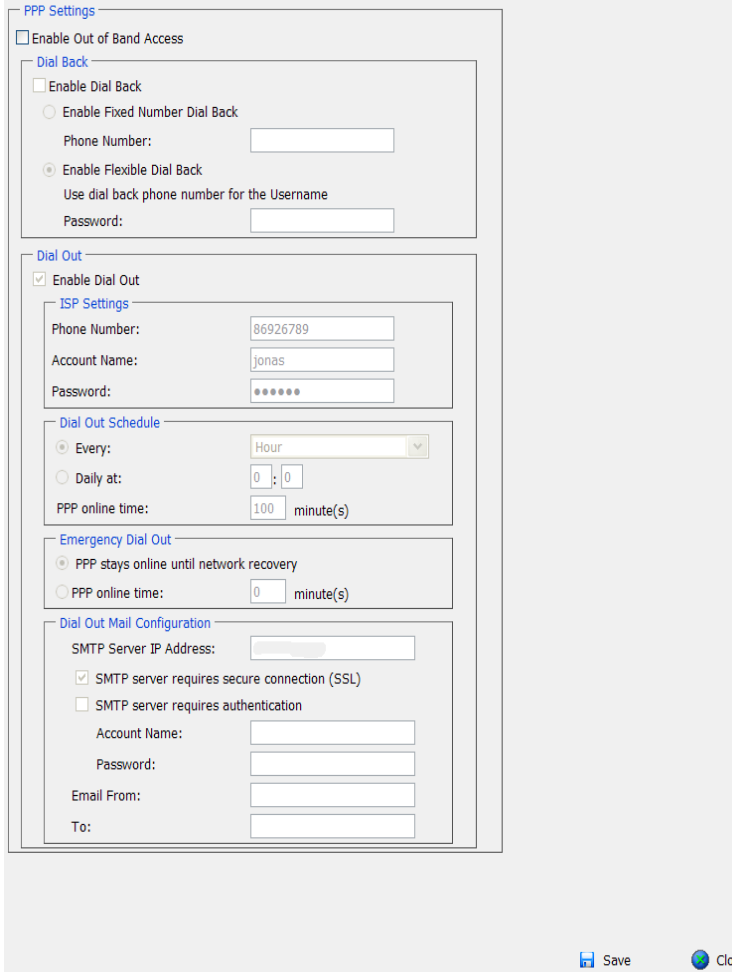


3. Select the Version.
4. Key in the Community Name.
5. Key in NMS IP/Host Name.
6. Select the Access Type and click **Save**.

OOBC

In case the KVM over IP switch cannot be accessed with the usual LAN-based methods, it can be accessed via the switch's modem port. To enable support for PPP (modem) operation, click to put a checkmark in the *Enable Out of Band Access* checkbox.

Note: See *PPP Modem Operation*, page 257, for PPP setup and operation.



When you enable Out of Band Access, the *Enable Dial Back*, and *Enable Dial Out* functions become available, as described in the sections that follow.

Enable Dial Back

As an added security feature, if this function is enabled, the switch disconnects the calls that dial in to it, and dials back to one of the entries specified in the table below:

Item	Action
Enable Fixed Number Dial Back	If *Fixed Number Dial Back* is enabled, when there is an incoming call, the KVM over IP switch hangs up the modem and dials back to the modem whose phone number is specified in the Phone Number field. Key the phone number of the modem that you want the KVM over IP switch to dial back to in the *Phone Number* field.
Enable Flexible Dial Back	If *Flexible Dial Back* is enabled, the modem that the KVM over IP switch dials back to doesn't have to be fixed. It can dial back to any modem that is convenient for the user, as follows: 1. Key the password that the users must specify in the *Password* field. 2. When connecting to the KVM over IP switch's modem, users specify the phone number of the modem that they want the KVM over IP switch to dial back to as their Username, and specify the password set in the *Password* field for their password.

Enable Dial Out

For the dial out function, you must establish an account with an Internet Service Provider, and use a modem to dial up to your ISP account. An explanation of the Enable Dial Out items is given in the table below:

Item	Action
ISP Settings	Specify the telephone number, account name (username), and password that you use to connect to your ISP.
Dial Out Schedule	This entry sets up the times you want the KVM over IP switch to dial out over the ISP connection. ◆ *Every* provides a listing of fixed times from every hour to every four hours. ◆ If you select *Every two hours* (for example), the KVM over IP switch will start dialing out every two hours beginning at 00:00. ◆ If you don't want the KVM over IP switch to dial out on a fixed schedule, select **Never** from the list. ◆ *Daily at* will dial out once a day at a specified time. Use the hh:mm format to specify the time. ◆ *PPP online time* specifies how long you want the ISP connection to last before terminating the session and hanging up the modem. A setting of zero means it is always on line.

Item	Action
Emergency Dial Out	If the KVM over IP switch gets disconnected from the network, or the network goes down, this function puts the switch on line via the ISP dial up connection. ◆ If you choose *PPP stays online until network recovery*, the PPP connection to the ISP will last until the network comes back up or the switch reconnects to it. ◆ If you choose *PPP online time*, the connection to the ISP will terminate after the amount of time that you specify is up. A setting of zero means it is always on line.
Dial Out Mail Configuration	This section provides email notification of problems that occur on the devices connected to the KVM over IP switch's ports (see *SMTP Settings*, page 162). **Note:** This email notification differs from the one configured under *SMTP Settings*, page 162, in that it uses the ISP mail server rather than the internal company's mail server. ◆ Key in the IPv4 address, IPv6 address, or domain name of your SMTP server in the SMTP Server IP Address field. ◆ Key in the email address of the person responsible for the SMTP server (or some other equally responsible administrator), in the Email From field. ◆ Key in the email address (addresses) of where you want the report sent to in the *To* field. If you are sending the report to more than one email address, separate the addresses with a comma or a semicolon. ◆ If your server requires a secure SSL connection, put a check in the *SMTP server requires secure connection (SSL)* checkbox ◆ If your server requires authentication, put a check in the *SMTP server requires authentication* checkbox, then key in the appropriate account name and password in the fields, below.

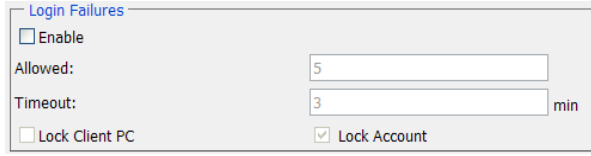
When you have finished making your settings on this page, click **Save**.

Security

The Security page is divided into 7 main panels, as described in the sections that follow.

Login Failures

For increased security, the Login Failures section allows administrators to set policies governing what happens when a user fails to log in successfully.

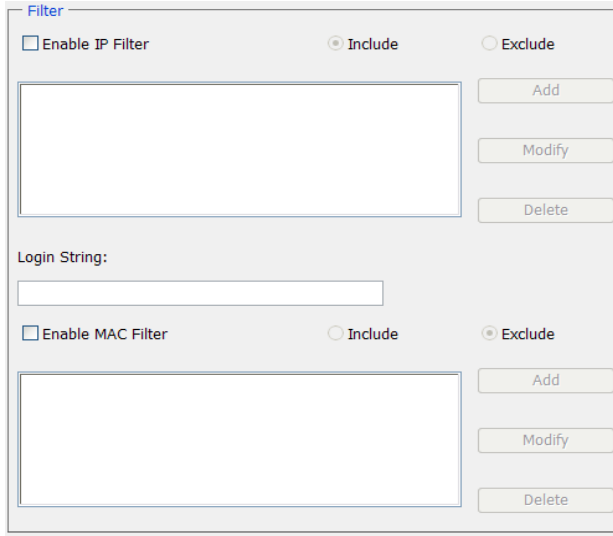


To set the Login Failures policy, check the *Enable* checkbox (the default is for Login Failures to be enabled). The meanings of the entries are explained in the table below:

Entry	Explanation
Allowed	Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5 times.
Timeout	Sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.
Lock Client PC	If this is enabled, after the allowed number of failures have been exceeded, the computer attempting to log in is automatically locked out. No logins from that computer will be accepted. The default is enabled. **Note:** This function relates to the client computer's IP. If the IP is changed, the computer will no longer be locked out.
Lock Account	If this is enabled, after the allowed number of failures have been exceeded, the user attempting to log in is automatically locked out. No logins from the username and password that have failed will be accepted. The default is enabled.

Note: If Login Failures is not enabled, users can attempt to log in an unlimited number of times with no restrictions. For security purposes, we recommend that you enable this function and enable the lockout policies.

Filter



- IP and MAC Filtering

  IP and MAC Filters control access to the KVM over IP switch based on the IP and/or MAC addresses of the client computers attempting to connect. A maximum of 100 IP filters and 100 MAC filters are allowed. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.

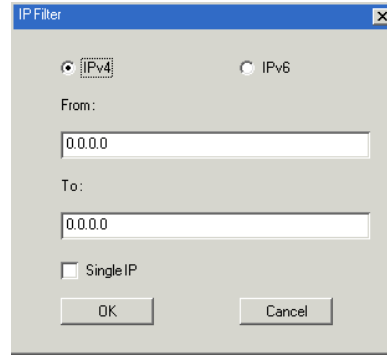
  To enable IP and/or MAC filtering, **Click** to put a check mark in the *IP Filter Enable* and/or *MAC Filter Enable* checkbox.

  - If the include button is checked, all the addresses within the filter range are allowed access; all other addresses are denied access.
  - If the exclude button is checked, all the addresses within the filter range are denied access; all other addresses are allowed access.

- Adding Filters

  To add an IP filter, do the following:

  1. Click **Add**. A dialog box similar to the one below appears:



  2. Specify whether you are filtering an IPv4 or IPv6 address.
  3. Key the address you want to filter in the *From:* field.
     - To filter a single IP address, click to put a check in the *Single IP* checkbox.
     - To filter a continuous range of addresses, key in the end number of the range in the *To:* field.

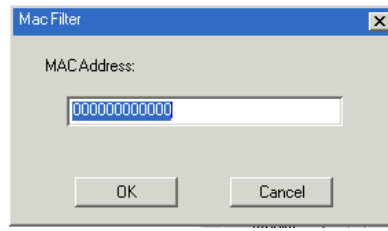
     Note: This description is for the AP GUI. The Browser GUI differs as follows:

     1. It doesn't offer an IPv4 or IPv6 choice. It only has *From* and *To* fields for IPv4 filtering.
     2. It doesn't have a checkbox to specify a single IP address. To filter a single IPv4 address, key the same address in both the *From* and *To* fields.

  4. After filling in the address, click **OK**.
  5. Repeat these steps for any additional IP addresses you want to filter.

To add a MAC filter, do the following:

1. Click **Add**. A dialog box similar to the one below appears:



2. Specify the MAC address in the dialog box, then click **OK**.
3. Repeat these steps for any additional MAC addresses you want to filter.

- IP Filter / MAC Filter Conflict

  If there is a conflict between an IP filter and a MAC filter – in other words, if a computer's address is allowed by one filter but blocked by the other – then the blocking filter takes precedence (the computer's access is blocked).

- Modifying Filters

  To modify a filter, select it in the IP Filter or MAC Filter list boxes and click **Modify**. The Modify dialog box is similar to the Add dialog box. When it comes up, simply delete the old address(es) and replace it with the new one(s).

- Deleting Filters

  To delete a filter, select it in the IP Filter or MAC Filter list box and click **Delete**.

Login String

The *Login String* entry field lets the super administrator specify a login string (in addition to the IP address) that users must add to the IP address when they access the KVM over IP switch with a browser.

For example, if *192.168.0.126* were the IP address, and *abcdefg* were the login string, then the user would have to key in:

```
192.168.0.126/abcdefg
```

Note: 1. Users must place a forward slash between the IP address and the string.

2. If no login string is specified here, anyone will be able to access the KVM over IP switch login page using the IP address alone. This makes your installation less secure.

The following characters are allowed in the string:

0–9 a–z A–Z ~ ! @ $ & * ( ) _ - = + [ ] .

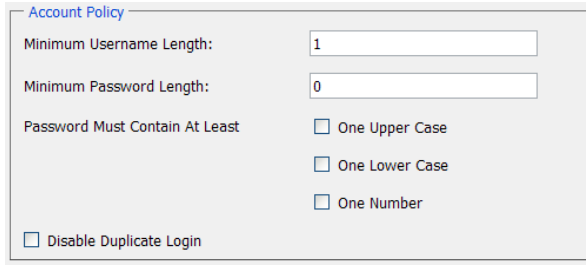
The following characters are not allowed:

% ^ ” : / ? # \ ‘ { } ; ’ < > [Space]
Compound characters (É Ç ñ ... etc.)

For security purposes, we recommend that you change this string occasionally.

Account Policy

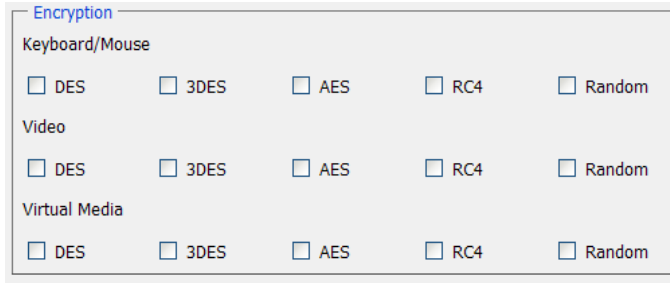
In the Account Policy section, system administrators can set policies governing usernames and passwords.



The meanings of the Account Policy entries are explained in the table below:

Entry	Explanation
Minimum Username Length	Sets the minimum number of characters required for a username. Acceptable values are from 1–16. The default is 6.
Minimum Password Length	Sets the minimum number of characters required for a password. Acceptable values are from 0–16. A setting of 0 means that no password is required. Users can login with only a Username. The default is 6.
Password Must Contain At Least	Checking any of these items requires users to include at least one uppercase letter, one lowercase letter or one number in their password. **Note:** This policy only affects user accounts created after this policy has been enabled, and password changes to existing user accounts. Users accounts created before this policy was enabled, and there is no change to the existing passwords, are not affected.
Disable Duplicate Login	Check this to prevent users from logging in with the same account at the same time.

Encryption

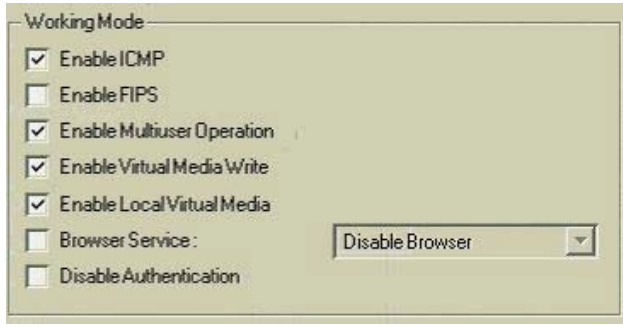


These flexible encryption alternatives for keyboard/mouse, video, and virtual media data let you choose any combination of DES; 3DES; AES; RC4; or a Random cycle of any or all of them.

Enabling encryption affects system performance – no encryption offers the best performance; the greater the encryption the greater the adverse effect. If you enable encryption, the performance considerations are as follows:

- RC4 offers the least impact on performance; DES is next; then 3DES or AES
- The RC4 + DES combination offers the least impact of any combination

Mode

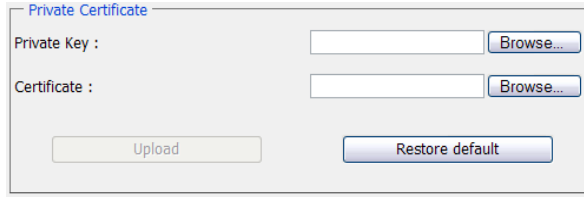


An explanation of the Mode items is given in the table, below:

Item	Explanation
Enable ICMP	If *ICMP* is **enabled**, the KVM over IP switch can be pinged. If it is not enabled, the device cannot be pinged. The default is Enabled.
Enable FIPS	Enables the FIPS security standard.
Enable Multiuser Operation	Enabling *Multiuser operation* permits up to 32 users to log in at the same time to share the remote bus. If not enabled, only one user can log in at a time. The default is Enabled.
Enable Virtual Media Write Operation	Enabling *Virtual Media Write Operation* allows redirected virtual media devices on a user's system to send data to a remote server, as well as being able to have data from the remote server written to them.
Enable Local Virtual Media	Enabling *Local Virtual Media* allows USB storage peripherals (CD/DVD, HD, flash drives, etc.) connected to the KVM over IP switch to appear and act as if it were installed on a remote system.
Browser Service	Enabling Browser Service allows the administrator to restrict browser access to the KVM over IP switch. After checking *Browser Service*, drop down the listbox to select the degree of restriction: **Disable Browser:** means no browser access is permitted. **Disable HTTP:** means browser access is permitted, but users must access the switch with an HTTPS URL. **Disable HTTPS:** means browser access is permitted, but users must access the switch with an HTTP URL.
Disable Authentication	If *Disable Authentication* is checked, no authentication procedures are used to check users attempting to log in. Users gain Administrator access to the KVM over IP switch simply by entering combination of username and password. **Note:** Enabling this setting creates an extremely dangerous result as far as security goes, and should only be used under very special circumstances.

Private Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the *Private Certificate* section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.



There are two methods for establishing your private certificate: generating a self-signed certificate; and importing a third-party certificate authority (CA) signed certificate.

- Generating a Self-Signed Certificate

  If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 272 for details about using OpenSSL to generate your own private key and SSL certificate.

- Obtaining a CA Signed SSL Server Certificate

  For the greatest security, we recommend using a third party certificate authority (CA) signed certificate. To obtain a third party signed certificate, go to a CA (Certificate Authority) website to apply for an SSL certificate. After the CA sends you the certificate and private encryption key, save them to a convenient location on your computer.

- Importing the Private Certificate

  To import the private certificate, do the following:

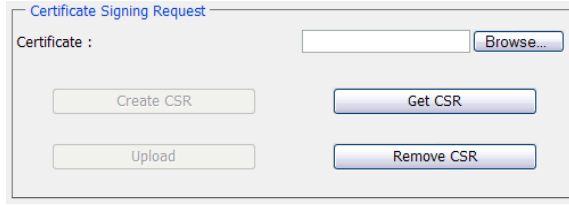
  1. Click **Browse** to the right of *Private Key*; browse to where your private encryption key file is located; and select it.
  2. Click **Browse** to the right of *Certificate*; browse to where your certificate file is located; and select it.
  3. Click **Upload** to complete the procedure.

Note: 1. Clicking **Restore Default** returns the device to using the default ATEN certificate.

2. Both the private encryption key and the signed certificate must be imported at the same time.

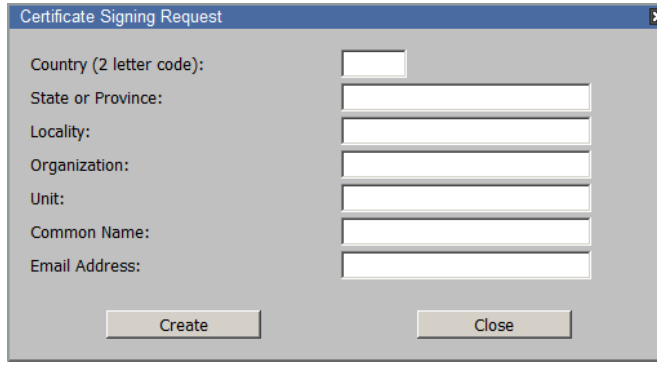
Certificate Signing Request

The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA signed SSL server certificate.



To perform this operation do the following:

1. Click **Create CSR**. The following dialog box appears:



2. Fill in the form – with entries that are valid for your site – according to the example information in the following table:

Information	Example
Country (2 letter code)	TW
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Techdoc Department
Common Name	mycompany.com **Note:** This must be the exact domain name of the site that you want the certificate to be valid for. If the site's domain name is *www.mycompany.com*, and you only specify *mycompany.com*, the certificate will not be valid.
Email Address	administrator@yourcompany.com

3. After filling in the form (all fields are required), click **Create**.

   A self-signed certificate based on the information you just provided is now stored on the KVM over IP switch.

4. Click **Get CSR**, and save the certificate file (*csr.cer*) to a convenient location on your computer

   This is the file that you give to the third party CA to apply for their signed SSL certificate.

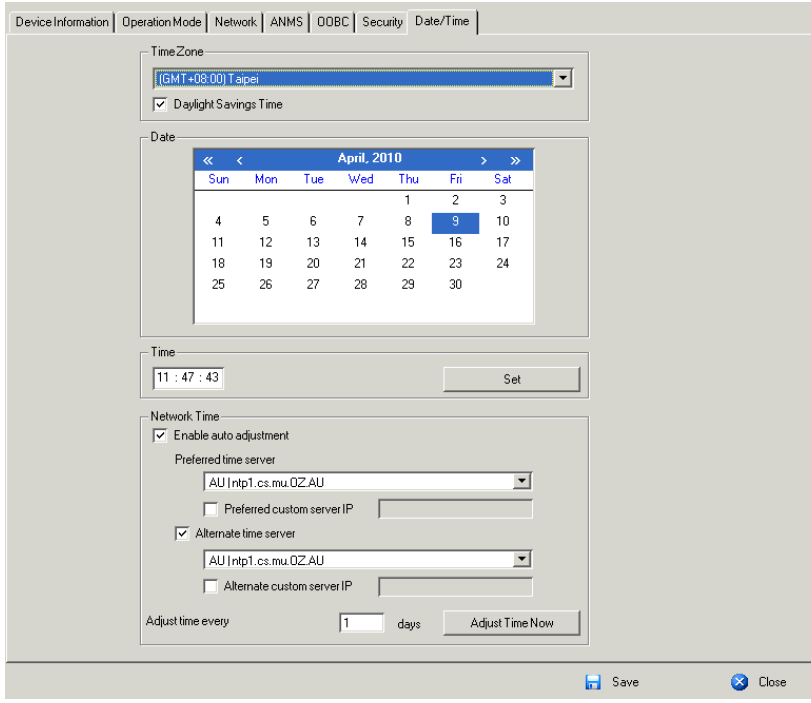
5. After the CA sends you the certificate, save it to a convenient location on your computer. Click **Browse** to locate the file; then click **Upload** to store it on the KVM over IP switch.

Note: When you upload the file, the KVM over IP switch checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

If you want to remove the certificate (to replace it with a new one because of a domain name change, for example), simply click **Remove CSR**.

Date/Time

The Date/Time dialog page sets the KVM over IP switch time parameters:



Set the parameters according to the information below.

Time Zone

- To establish the time zone that the KVM over IP switch is located in, drop down the *Time Zone* list and choose the city that most closely corresponds to where it is at.
- If your country or region employs Daylight Saving Time (Summer Time), check the corresponding checkbox.

Date

- Select the month from the drop down listbox.
- Click < or > to move backward or forward by one year increments.
- In the calendar, click on the day.
- To set the time, use the 24 hour HH:MM:SS format.
- Click **Set** to save your settings.

Network Time

To have the time automatically synchronized to a network time server, do the following:

1. Check the *Enable auto adjustment* checkbox.
2. Drop down the time server list to select your preferred time server

   – or –

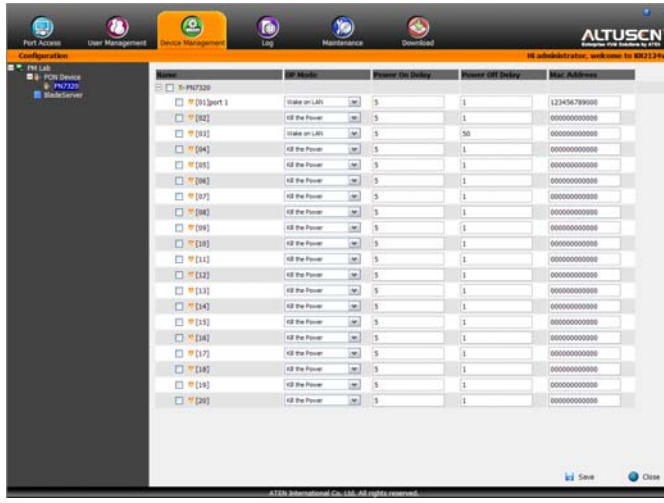
   Check the *Preferred custom server IP* checkbox, and key in either the IPv4 address, IPv6 address, or domain name of the time server of your choice.
3. If you want to configure an alternate time server, check the *Alternate time server* checkbox, and repeat step 2 for the alternate time server entries.
4. Key in your choice for the number of days between synchronization procedures.
5. If you want to synchronize immediately, click **Adjust Time Now**.

PON Devices

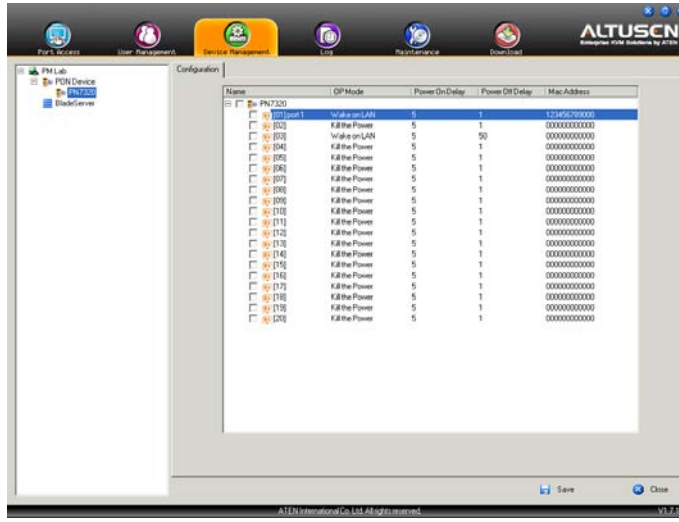
Configuration Page

When a PON device is selected in the Sidebar, its *Configuration* page comes up:

Browser GU



AP GUI



Outlet Configuration

The outlet configuration settings that can be made on this page are the same ones described under *Power Management*, in the table on page 132.

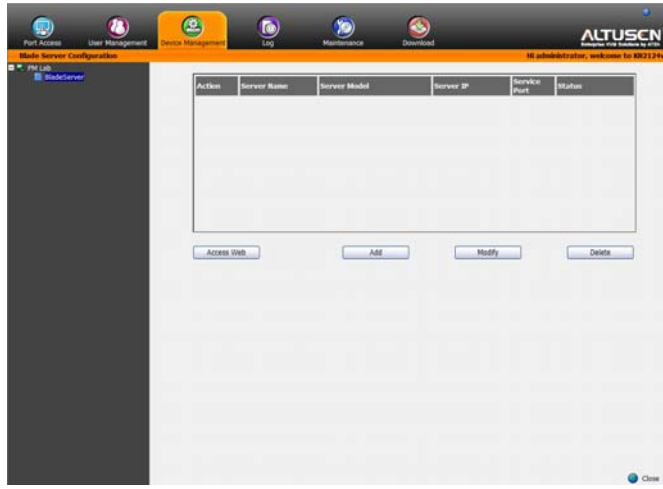
- Click on a setting to drop down the list of choices.
- To give more than one outlet the same setting at the same time, click to put a check mark in front of the outlets you want to configure. When you change the setting for any one of the outlets, each of the selected outlets will get the new setting.
- To change the setting for all of the outlets at the same time, click to put a check mark in front of the PON's name. All of the outlets are selected. When you change the setting for any one of the outlets, all of the outlets will get the new setting.

Blade Servers

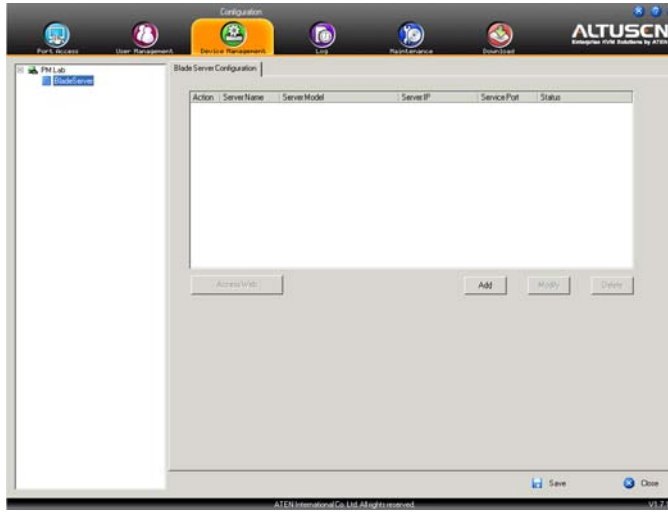
Configuration Page

For Super Administrators, when a Blade Server is selected in the Sidebar, its *Configuration* page comes up:

Browser GUI



AP GUI

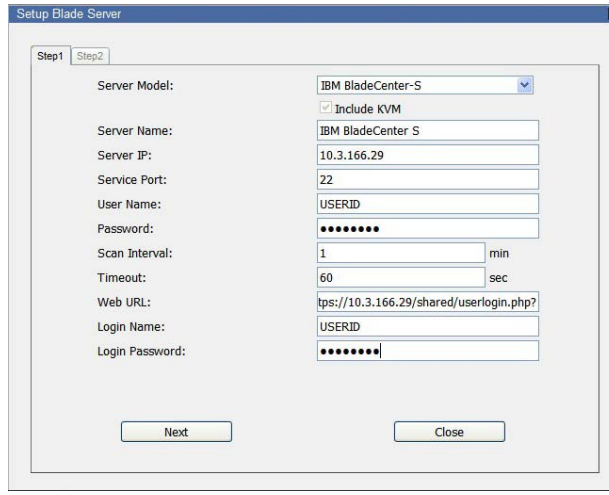


Blade Server Setup

Adding a Blade Server

To configure a new Blade server, do the following:

1. Select its icon in the Sidebar, then click **Add** in the main panel. The *Setup Blade Server* dialog box comes up, with the *Step 1* tab displayed:



2. Fill in the fields according to the information provided in the table, below:

Field	Explanation
Server Model	Drop down the list to select the blade server chassis model. If your model isn't included in the list of supported servers, contact your dealer for help.
Include KVM	This item is for information purposes and can't be edited. If the server supports a KVM function, this box is checked. Otherwise, it is unchecked.
Server Name	For convenience, you can give the server a name.
Server IP	Key in the server's IP address (IPv4, IPv6, or domain name) used to access the server via a serial connection (Telnet or SSH)
Service Port	Key in the port number used for serial access.
User Name	Key in the username required for serial access authentication.
Password	Key in the password required for serial access authentication.
Scan Interval	The interval between times that the KVM over IP switch scans the server for information.

Field	Explanation
Timeout	The amount of time that the KVM over IP switch waits for a response from the server before it stops scanning for information.
Web URL	Key in the server's IP address (IPv4, IPv6, or domain name) used to access the server via a browser.
Login Name	Key in the username required for browser authentication.
Login Password	Key in the password required for browser authentication.

3. When you have finished configuring the fields, click **Next** to bring up the dialog box with the *Step 2* tab displayed.
4. The *Step 2* dialog presents a summary of the blade server's configuration, including the number of blades installed. Click **Save** to add the blades server to the installation.

Modifying / Deleting a Blade Server

- To modify a blade server's configuration, first select it in the Sidebar, then click **Modify**. Make your changes on the *Setup Blade Server* dialog box.
- To remove a blade server, first select it in the Sidebar, then click **Delete**.

Web Access

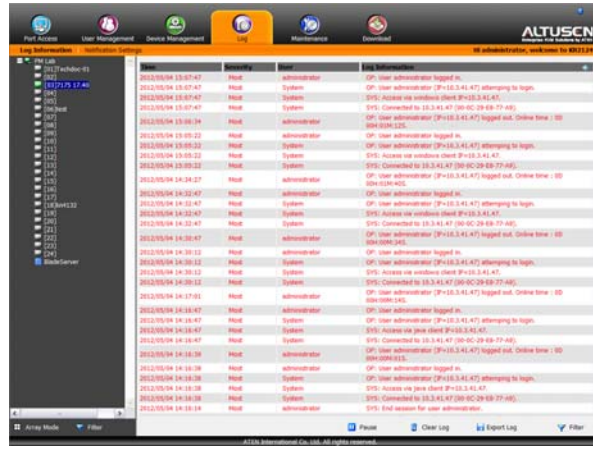
To access the blade server's Web page, first select it in the Sidebar, then click **Access Web**.

Chapter 9
Log

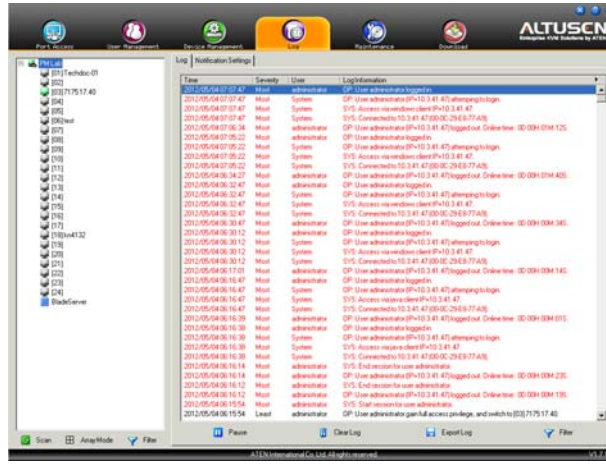
Overview

The KVM over IP switch logs all the events that take place on it. To view the contents of the log, click the *Log* tab. The device's Log Information page, similar to the one below, appears:

Browser GUI



AP GUI



Log Information

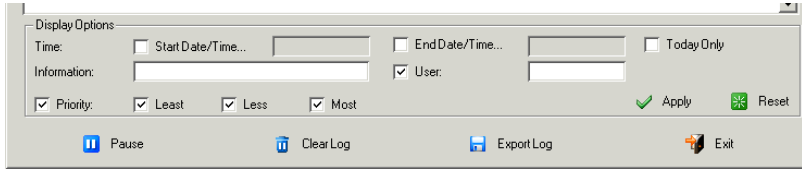
The Log Information page displays events that take place on the KVM over IP switch, and provides a breakdown of the time, the severity, the user, and a description of each one. You can change the sort order of the display by clicking on the column headings.

The log file tracks a maximum of 512 events. When the limit is reached, the oldest events get discarded as new events come in. The purpose of the buttons at the bottom of the page are described in the following table:

Button	Explanation
Pause	Clicking *Pause* stops the display of new events. When the display is paused the button changes to *Resume*. Click **Resume** to start displaying events again.
Clear Log	Clicking *Clear Log* clears the log file.
Export Log	Clicking *Export Log* lets you save the contents of the log to a file on your computer.
Filter	Clicking *Filter* allows you to search for particular events by date or by specific words or strings, as described in the next section.

Filter

Filter lets you narrow the log event display to ones that occurred at specific times; ones containing specific words or strings; or ones involving specific users. When you access this function, the log filter dialog box appears at the bottom of the page:

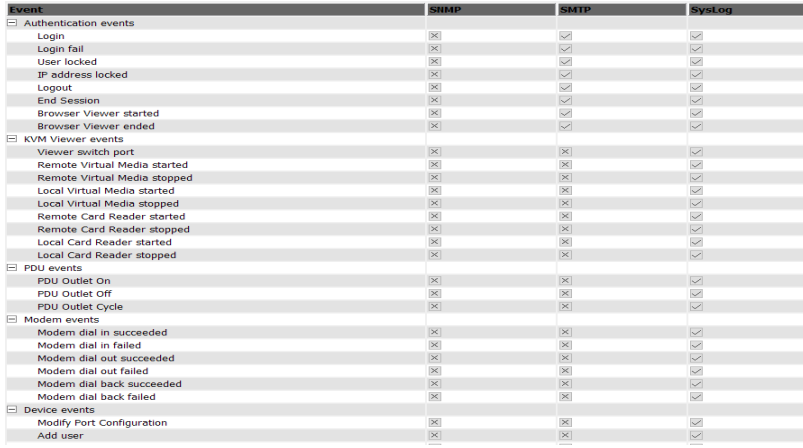


A description of the filter items is given in the table, below:

Item	Description
Time	This feature lets you filter for events that occurred at specific times, as follows: **Today Only:** Only the events for the current day are displayed. **Start Date/Time:** Filters for events from a specific date and time to the present. Put a check in the checkbox to bring up a calendar. Set the date and time that you want the filtering to start from. All events from the Start date/time to the present are displayed. For the Web Browser interface, after checking Start Date/Time, you have to click inside the text box in order to bring up the calendar. When you have made your calendar choices, click the **A** icon at the lower right of the calendar panel. **End Date/Time:** Filters for events from a specific date and time to a specific date and time. First select the Start Date/Time (described above); check **End Date/Time** to set the ending date and time. For the Web Browser interface, after checking End Date/Time, you have to click inside the text box in order to bring up the calendar. When you have made your calendar choices, click the **A** icon at the lower right of the calendar panel.
Information	Filters for a particular word or string. Key the word or string into the *Information* text box. Only events containing that word or string are displayed. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
User	Filters for specific users. First put a check in the *User* checkbox; then key in the user's Username; then click **Apply**. Only events containing that Username are displayed. **Note:** If the *User* checkbox is not checked here in the Filter panel, the entire User column does not appear in the main panel.
Severity	Filters based on the severity rating of the event. Least events appear in black; Less events appear in blue; Most events appear in red. First put a check in the *Severity* checkbox; then check the severity options you want to filter for (you can check more than one item). Only events that match the severity ratings you specified appear in the display. **Note:** If the *Severity* checkbox is not checked here in the Filter panel, the entire Severity column does not appear in the main panel.
Apply	Click to apply the filter choices.
Reset	Click this button to clear the entries in the dialog box and start with a clean slate.
Exit	Click this button to exit the log filter function.

Log Notification Settings

The Notification Settings page lets you decide which events trigger a notification, and how the notification are sent out:



Event	SNMP	SMTP	SysLog
Authentication events			
Login	☒	☑	☑
Login fail	☒	☑	☑
User locked	☒	☑	☑
IP address locked	☒	☑	☑
Logout	☒	☑	☑
End Session	☒	☑	☑
Browser Viewer started	☒	☑	☑
Browser Viewer ended	☒	☑	☑
KVM Viewer events			
Viewer switch port	☒	☒	☑
Remote Virtual Media started	☒	☒	☑
Remote Virtual Media stopped	☒	☒	☑
Local Virtual Media started	☒	☒	☑
Local Virtual Media stopped	☒	☒	☑
Remote Card Reader started	☒	☒	☑
Remote Card Reader stopped	☒	☒	☑
Local Card Reader started	☒	☒	☑
Local Card Reader stopped	☒	☒	☑
PDU events			
PDU Outlet On	☒	☒	☑
PDU Outlet Off	☒	☒	☑
PDU Outlet Cycle	☒	☒	☑
Modem events			
Modem dial in succeeded	☒	☒	☑
Modem dial in failed	☒	☒	☑
Modem dial out succeeded	☒	☒	☑
Modem dial out failed	☒	☒	☑
Modem dial back succeeded	☒	☒	☑
Modem dial back failed	☒	☒	☑
Device events			
Modify Port Configuration	☒	☒	☑
Add user	☒	☒	☑

Notifications can be sent via SNMP trap, SMTP email, written to the SysLog file, or any combination of the three. A check mark (√) indicates that notification of the event is enabled for the method specified in the column heading; an X indicates that notification is not enabled.

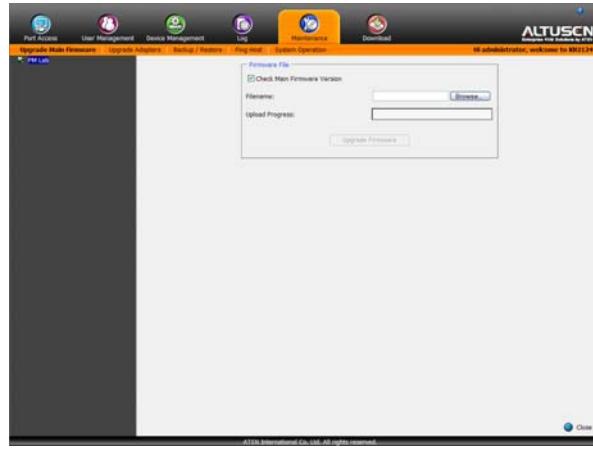
Note: In any of the columns, you can use Shift-Click or Ctrl-Click to select a group of events. Clicking to enable/disable any one of them causes all of them to change in unison.

Chapter 10
Maintenance

Overview

The *Maintenance* function is used to upgrade firmware; backup and restore configuration and account information; ping network devices; and restore default values.

Browser GUI



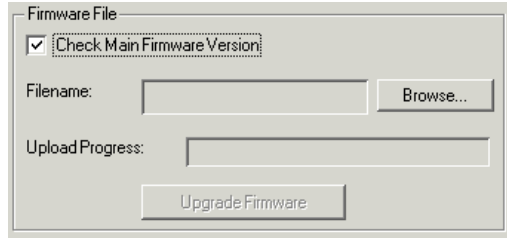
AP GUI

Main Firmware Upgrade

In addition to upgrading the KVM over IP switch's main firmware, this function can also be used to upgrade any PON units and Blade Servers deployed on the installation. As new versions of the firmware become available, they can be downloaded from our website. Check the website regularly to find the latest information and packages.

To upgrade the main firmware, do the following:

1. Download the new firmware file (switch, PON or blade server module), to your computer.
2. Log in to the KVM over IP switch; and click the *Maintenance* tab. The Maintenance tab opens to the *Upgrade Main Firmware* page:



3. Click **Browse**; navigate to the directory that the new firmware file is in and select the file.
4. Click **Upgrade Firmware** to start the upgrade procedure.
   - If you enabled *Check Main Firmware Version* the current firmware level is compared with that of the upgrade file. If the current version is equal to or higher than the upgrade version, a popup message appears, to inform you of the situation and stops the upgrade procedure.
   - If you didn't enable *Check Main Firmware Version*, the upgrade file is installed without checking what its level is.
   - As the upgrade proceeds, progress information is shown in the *Progress* bar.
   - Once the upgrade completes successfully, the switch resets itself.
5. Log in again, and check the firmware version to be sure it is the new one.

Note: To recover from a "failed upgrade" situation, see *Firmware Upgrade Recovery*, page 197.

Firmware Upgrade Recovery

Should the switch's main firmware upgrade procedure fail, and the switch becomes unusable, the following firmware upgrade recovery procedure will resolve the problem:

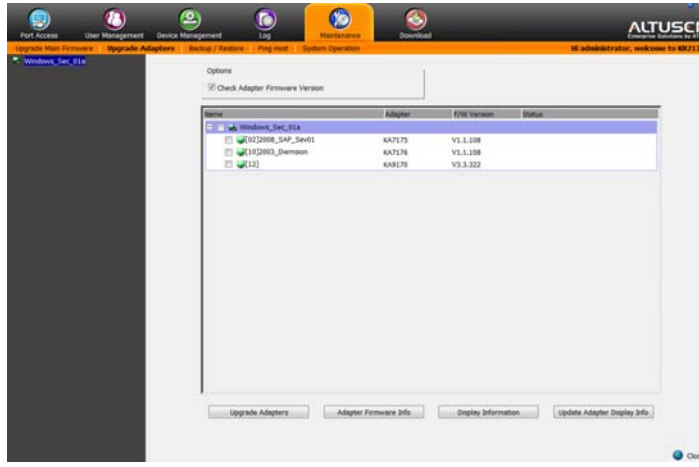
1. Power off the switch.
2. Press and hold the Reset Switch in (see *Reset Switch*, page 11).
3. While holding the Reset Switch in, power the switch back on.

This causes the switch to use the original factory installed main firmware version. Once the switch is operational, you can try upgrading the main firmware again by logging on to the KVM over IP switch via web browser (see *Main Firmware Upgrade*, page 196).

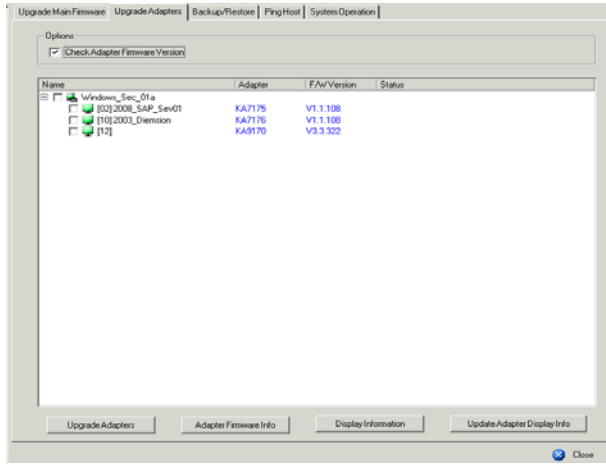
Upgrade Adapters

The *Upgrade Adapters* page allows you to view and update KVM adapter firmware and display information. This section refers to the KVM adapter cables that provide the EDID display information to the connected server, which allow its video to be displayed on the local console monitor.

Browser GUI



AP GUI



Upgrade Adapters

The *Upgrade Adapters* button is used to upgrade the firmware of the KVM Adapter Cables.

To perform the upgrades, do the following:

1. Click the *Maintenance* tab; select the *Upgrade Adapters* menu item.
2. Click **Adapter Firmware Info** to bring up a list of the adapter firmware versions that are stored in the main firmware. If you upgraded the main firmware, it may contain newer versions of the adapter firmware than the versions currently on the adapters.
3. Compare the adapter firmware versions stored in the main firmware with the versions listed in the *F/W Version* column of the Main Panel. If the versions stored in the firmware are newer than the ones on the adapters, you will probably want to perform the adapter upgrade.
4. In the *Name* column of the Main Panel, check the ports whose Adapters you want to upgrade.
5. Click **Upgrade Adapters** to start the upgrade procedure.
   - If you enabled *Check Adapter Firmware Version,* the current firmware level(s) are compared with that of the upgrade versions. If the current version is equal to, or higher than the upgrade version, a message appears in the adapters *Progress* column informing you that no upgrade is available and stops the upgrade procedure.
   - If you didn't enable *Check Adapter Firmware Version,* the upgrade files are installed without checking what their level is.
   - When the procedure completes the new adapter firmware version displays.

Note: 1. The switch may work with older adapter firmware versions, but for optimum compatibility we recommend upgrading your Adapter Cable firmware to that stored with the switch's Main firmware.

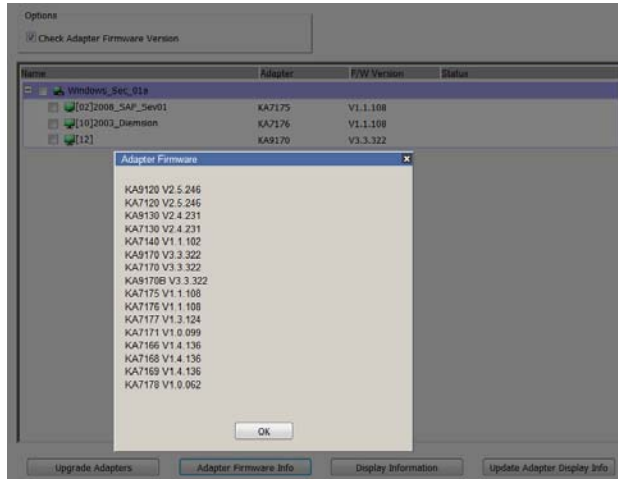
2. You can perform the upgrade procedure anytime you add an Adapter to the installation to make sure it is working with the latest firmware version.

3. To recover from a "failed upgrade" situation, see *Adapter Firmware Upgrade Recovery*, page 202.

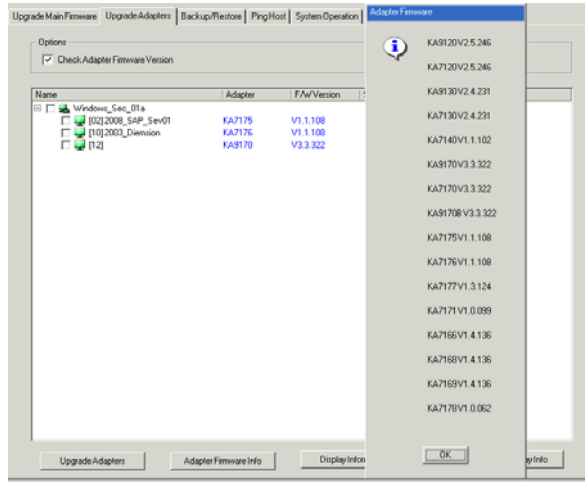
Adapter Firmware Info

The *Adapter Firmware Info* button provides a list of the Adapter Cable firmware stored on the switch's Main firmware. You can use this information to compare it to the *F/W Version* listed for the connected Adapter Cables. For optimum compatibility we recommend upgrading your Adapter Cable's firmware to match that stored with the switch's Main firmware.

Browser GUI

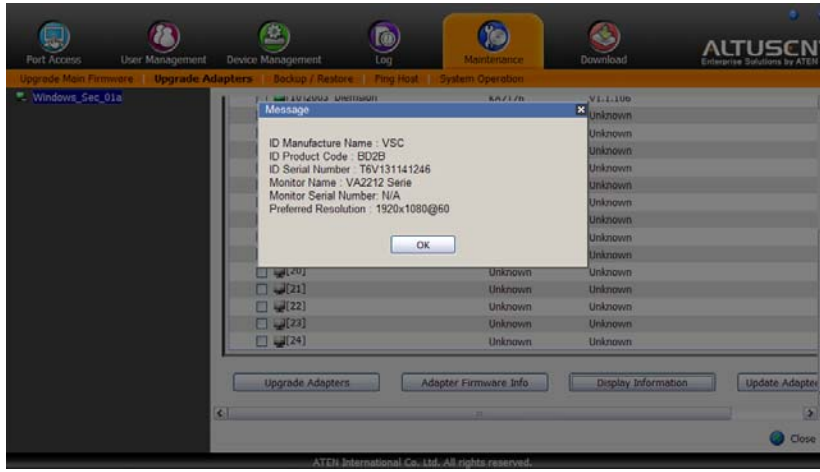


AP GUI



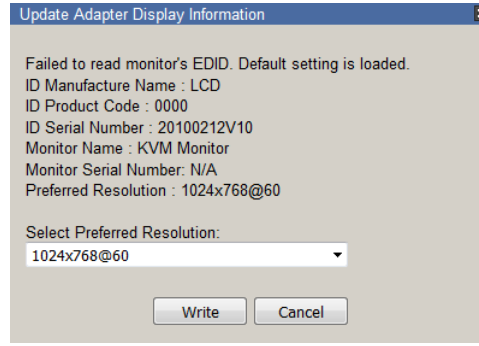
Display Information

The *Display Information* button will query and show the locally connected monitor's EDID information, as shown here:



Update Adapter Display Info

The *Update Adapter Display Info* button will query the local monitor's EDID information and update it on the Adapter Cable. The EDID information tells the server's video card about the hardware of the display it is connected to; in this case the monitor connected to the KVM console.



Use the *Display Information* button to obtain the local monitor's Preferred Resolution (optional), and apply it with the *Select Preferred Resolution* drop down menu, then click **Write**. If the local console is not connected to a monitor, the default EDID setting is loaded on the adapter cable.

Adapter Firmware Upgrade Recovery

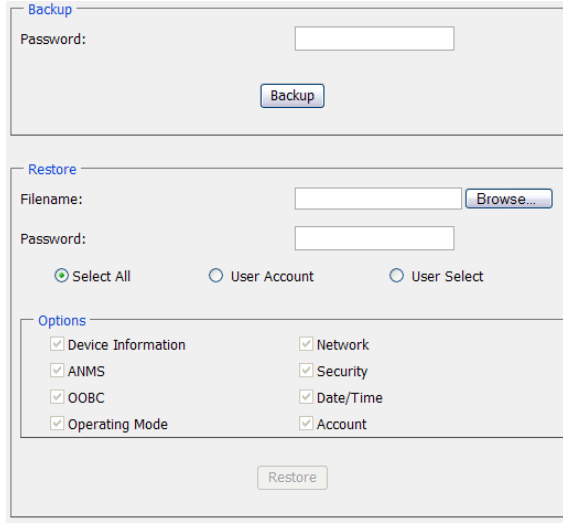
Should the adapter firmware upgrade procedure fail for one of the KVM Adapter Cables and the adapter becomes unusable, the following adapter firmware upgrade recovery procedure will resolve the problem:

1. Unplug the Adapter from the server it is connected to.
2. Slide its *Firmware Upgrade Recovery Switch* (located next to the Cat 5e connector) to the **RECOVER** position.
3. Plug the Adapter back into the server.
4. Repeat the Adapter upgrade procedure.

After the Adapter has been successfully upgraded, unplug the Adapter from the server it is connected to; slide the Firmware Upgrade Recovery Switch back to the **NORMAL** position; and plug the Adapter back in.

Backup/Restore

Selecting the Backup/Restore menu item gives you the ability to back up the switch's configuration and user profile information:



Backup

To backup the device's settings do the following:

1. In the *Password* field, key in a password for the file.

Note: 1. Setting a password is optional. If you do not set one, the file can be restored without specifying a password.

2. If you do set a password, make a note of it, since you will need it to be able to restore the file.

2. Click **Backup**.
3. When the browser asks what you want to do with the file, select *Save to disk*; then save it in a convenient location.

Restore

To restore a previous backup, do the following:

1. Click **Browse**; navigate to the file and select it.

   Note: If you renamed the file, you can leave the new name. There is no need to return it to its original name.

2. If you set a password when you created the file, key it in the *Password* field.
3. Select as many of the options that are presented as you wish to restore.
4. Click **Restore**.

   After the file is restored, a message appears to inform you that the procedure succeeded.

Terminal

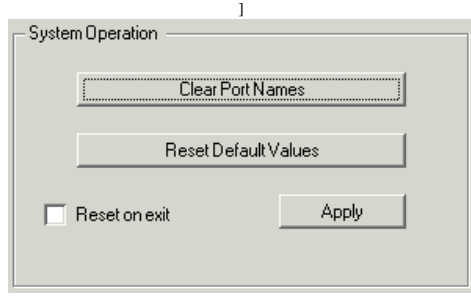
Terminal is also available for access to more advanced instructions through a terminal-like interface.

Available commands include:

- BLADEDEBUG => Debug blade server.
- CLS => Clears the screen.
- ENABLERC4 => Enable RC4 cipher.
- ENABLESSLV2 => Enables SSLv2 protocol.
- ENABLESSLV3 => Enables SSLv3 protocol.
- GET => Gets current configuration.
- HELP => Provides Help information for commands.
- LDAPDEBUG => Debugs ldap communication.
- NETINFO => Displays network statistics information.
- PING => Displays ping host information.
- SETLDAPMEMBER => Sets new value for ldap member.
- SETLDAPMEMBEROF => Sets new value for ldap memberof.
- SETPROMPT => Sets prompt string.
- SETSSLCIPHER => Sets SSL cipher strength.
- SOCKINFO => Displays socket connection information.
- TRACERT => Displays trace route information.

Restore Values

The Restore Values page lets you restore certain configuration changes that were made to the KVM over IP switch back to their original factory default values.



The functions performed on this page are as follows:

Clear Port Names:

Clicking this button removes names that have been assigned to the ports

Restore Default Values:

Clicking this button undoes all Customization page changes that have been made to the KVM over IP switch (except for the Port Names), as well as the Network Transfer Rate (on the Network page), and returns the parameters to the original factory default settings.

Reset on exit:

Place a check here and click **Apply** to have the KVM over IP switch reset itself and implement all the new settings when you log out. (Following the reset, wait approximately 30 to 60 seconds before logging back in.)

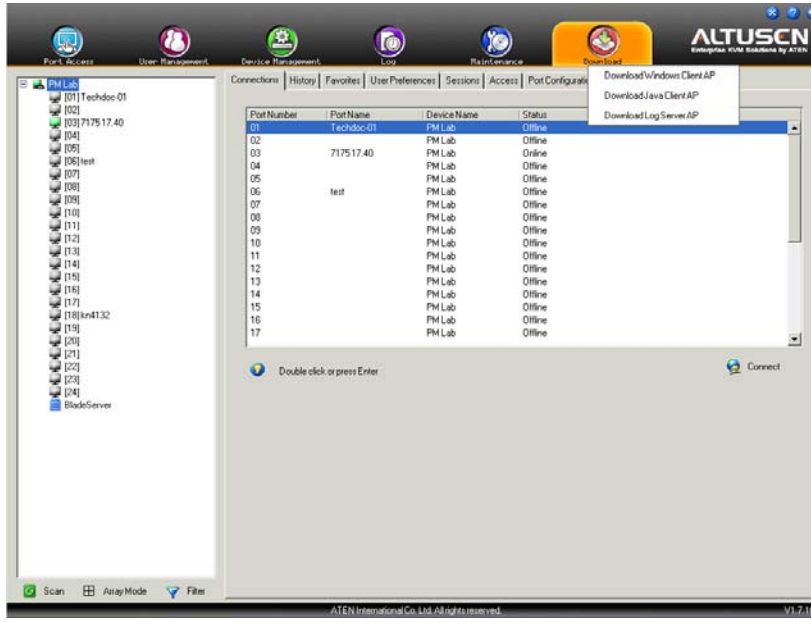
If you change the switch's IP Address (see *Network*, page 157), the checkbox is automatically checked and the KVM switch will reset when you log out. If you clear the check mark before logging out, the changed IP settings will be ignored and the original IP address settings will remain in effect.

Note: Even though the changed IP settings are ignored, they still remain in the network settings fields. Which means that the next time you open this page the *Reset on exit* checkbox will automatically be enabled, and when the switch resets, the new IP settings that you thought you discarded will become the ones used by the switch. To avoid this problem, you should go back to the network settings page and be sure that the IP settings that appear in the fields are the ones you want to use.

Chapter 11
Download

Overview

Download is used to download stand-alone AP versions of the Windows Client, the Java Client, and the Log Server:



Click the program you want to download; save it to a convenient location on your hard disk, and run it from there.

This Page Intentionally Left Blank

Chapter 12
Port Operation

Overview

After you have successfully logged in (see *Logging In*, page 43), the KVM over IP switch opens to the Port Access tab's Connections page, with the first KVM over IP switch selected in the sidebar:

Note: 1. The WinClient and Java Client AP programs have a hidden Control Panel at the upper center of the screen that becomes visible when you mouse over it. The Browser version's Control Panel only appears after you switch to a port. The Control Panel is discussed on page 59.

2. See *KVM Devices and Ports – Connections Page*, page 101 for details about the Port Access *Connections* page.

Connecting to a Port

All the devices, ports, and outlets that a user is permitted to access are listed in the Sidebar at the left of the page.

- To connect to a port when a device is selected in the Sidebar, double click its icon in the Sidebar; or double click anywhere on its line entry in the main central panel; or select it in the main panel and click **Connect** at the bottom right of the page.
- To connect to a port when the port is selected in the Sidebar, click **Connect** at the right of the *Status* panel (see *Status*, page 102).

Once you switch to a port, its screen displays on your monitor, and your keyboard and mouse input affects the remote server:

The Port Toolbar

The KVM over IP switch's interface provides a toolbar to help you with port switching operations from within the captured port. To bring up the toolbar, tap the GUI Hotkey (Scroll Lock or Ctrl), twice. The toolbar appears at the upper left corner of the screen:

Depending on the settings that were selected for ID Display (see page 117), the Port Number and/or the Port Name display at the right of the toolbar. The meanings of the toolbar icons are given in a table on page 212.

When the toolbar displays mouse and keyboard input has no effect on the server connected to the port. To carry out operations on the server, close the toolbar by clicking its **X** icon.

To return to the Port Access *Connections* page, either click the appropriate icon (see *The Toolbar Icons*, page 212), or tap the GUI hotkey again.

Note: 1. You can adjust the toolbar transparency (see *Video Settings*, page 73).

2. The toolbar functions and icons are also incorporated in the Control Panel. If you choose to enable them in the Control Panel (see *Control Panel Configuration*, page 90), you can disable the Toolbar (see *User Preferences*, page 117 for details). To recall the Port Access *Connections* page when there is no Toolbar, simply tap the GUI hotkey twice.

The Toolbar Icons

The meanings of the toolbar icons are explained in the table below.

Icon	Purpose
	Click to skip to the first accessible port on the entire installation, without having to recall the Port Access page.
	Click to skip to the first accessible port previous to the current one, without having to recall the Port Access page.
	Click to begin Auto Scan Mode. The KVM over IP switch automatically switches among the ports that were selected for Auto Scanning with the *Filter* function (see *Filter*, page 97). This allows you to monitor their activity without having to switch among them manually.
	Click to skip from the current port to the next accessible one, without having to recall the Port Access page.
	Click to skip from the current port to the last accessible port on the entire installation, without having to recall the Port Access page.
	Click to recall the Port Access page.
	Click to close the toolbar.
	Click to invoke Panel Array Mode (see *Panel Array Mode*, page 216).

Toolbar Hotkey Port Switching

When the toolbar displays, you can use hotkeys to provide KVM focus to a port directly from the keyboard. The KVM over IP switch provides the following hotkey features:

- Going directly to a port by keying in its port number and clicking **Enter**.
- Auto Scanning
- Skip Mode Switching

The hotkeys are: **A** and **P** for Auto Scanning; and the **Arrow Keys** for Skip Mode.

Note: 1. In order for hotkey operations to take place, the toolbar must be visible (see *The Port Toolbar*, page 211).

2. To use the keys designated as hotkeys (i.e. A, P, etc.) for normal, non-hotkey purposes, you must first close the toolbar.

3. For issues affecting multiple user operation in Auto Scan Mode, see *Multiuser Operation*, page 218.

Auto Scanning

The Scan function automatically switches among all the ports that are accessible to the currently logged on user at regular intervals, so that the user can monitor their activity automatically. Users can also limit the number of ports scanned with the Filter function of the Sidebar. See *KVM Devices and Ports – Connections Page*, page 101, and *Filter*, page 97, for further details.

- Setting the Scan Interval:

  The amount of time Auto Scan dwells on each port is set with the *Scan Duration* setting (see *Scan Duration*, page 118).

- Invoking Auto Scan

  To start Auto Scanning, with the toolbar showing, tap the **A** key. The Auto Scan function cycles through the ports in order – starting from the first port on the installation. An **S** appears in front of the Port ID Display to indicate that the port is being accessed under Auto Scan Mode.

- Pausing Auto Scan

  While you are in Auto Scan Mode, you can pause the scanning in order to keep the focus on a particular server by pressing **P**. During the time that Auto Scanning is paused, the **S** in front of the Port ID blinks On and Off.

  Pausing when you want to keep the focus on a particular server can be more convenient than exiting Auto Scan Mode because when you *Resume* scanning, you start from where you left off. If, on the other hand, you were to exit and then restart Auto Scan Mode, the scanning would start over from the very first server on the installation.

  To *Resume* Auto Scanning after a pause, press any key except [Esc] or the [Spacebar]. Scanning continues from where it left off.

- Exiting Auto Scan

  While Auto Scan Mode is in effect, ordinary keyboard functions are suspended. You must exit Auto Scan Mode in order to regain normal control of the keyboard. To exit Auto Scan Mode press [Esc] or the [Spacebar]. Auto Scanning stops when you exit Auto Scan Mode.

Skip Mode

Skip Mode allows you to switch ports in order to monitor the servers manually. You can dwell on a particular port for as long or as little as you like - as opposed to Auto Scanning, which automatically switches after a fixed interval. The Skip Mode hotkeys are the four Arrow keys. Their operation is explained in the table below:

Arrow	Action
←	Skips from the current port to the first accessible port previous to it.
→	Skips from the current port to the first accessible port that comes after it.
↑	Skips from the current port to the very first accessible port on the installation.
↓	Skips from the current port to the very last accessible port on the installation.

Recalling the Port Access Page

To dismiss the toolbar and bring back the Port Access page, do one of the following:

- Tap the GUI Hotkey once.
- From the toolbar, click the icon that recalls the Port Access page (see *The Toolbar Icons*, page 212).

The toolbar closes, and the Port Access Page appears.

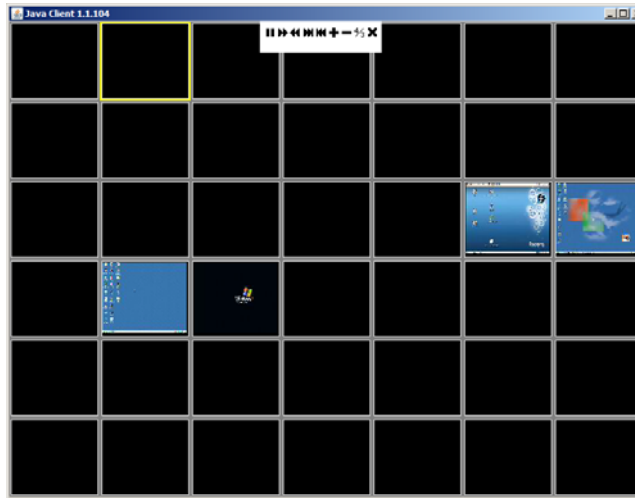
GUI Hotkey Summary Table

The following table presents a summary of the GUI Hotkey actions after you have accessed a port. See *User Preferences*, page 117 to set the GUI Hotkey.

To...		Do This...
Open the Toolbar		Click the GUI Hotkey twice
Open the Port Access Page	The Toolbar is open	Click the GUI Hotkey once
	The Toolbar is not open	Click the GUI Hotkey three times

Panel Array Mode

Clicking the toolbar's *Panel* icon invokes Panel Array Mode. Under this mode, the screen divides into a grid of up to 42 panels:



- Each panel represents one of the switch's ports beginning with Port 1 at the upper left, and going from left to right; top to bottom.
- The number of panels in the array can be selected by clicking the **Show More Ports**, and **Show Fewer Ports** symbols on the panel array toolbar (see the following page for an explanation of the panel array toolbar).
- When the Array is first invoked, it scans through each of the ports that were selected for Auto Scanning with the *Filter* function (see *Filter*, page 97). As it scans, the border of the panel that has the focus becomes highlighted.
- Only ports that are accessible to the user are displayed. For ports that are not accessible, the panel is blank.
- If the server connected to a port is on line, its screen displays in its panel, otherwise the panel is blank.
- Mousing over a panel displays information about the port (port name, online status, port access status, and resolution).
- You can access a server connected to a port by moving the mouse pointer over its panel and clicking. You switch to the server exactly as if you had selected it from the Port Access page.

Panel Array Toolbar

The panel array toolbar provides shortcut navigation and control of the panel array. The toolbar can be dragged anywhere on the screen. Mousing over an icon brings up a “tooltip” that provides a short description of the icon’s function. The icon functions are described in the table below:

	Click and drag to move the toolbar. **Note:** This icon is only available with the Windows Clients. To move the Java Client toolbars, click on any empty space and drag.
	Pause panel scanning, leaving the focus on the panel that currently has it.
	Move back four panels.
	Move to the previous panel.
	Move to the next panel.
	Move ahead four panels.
	Show More Ports: Increase the number of panels in the array.
	Show Fewer Ports: Decrease the number of panels in the array.
	Toggle 4/3 aspect ratio.
	Exit Panel Array mode.

Note: For issues affecting multiple user operation in Panel Array Mode, see *Multiuser Operation*, page 218.

Multiuser Operation

The KVM over IP switch supports multiuser operation. When multiple users simultaneously access the switch from client computers, the rules of precedence that apply are shown in the following table:

Operation	Rule
General	Each bus is independent. For an explanation of the method by which users are assigned to buses, see the next section, *Users and Buses*. Each user can open his own independent GUI Main Page.
Auto Scan Mode	If a user has invoked Auto Scan Mode (see page 213), and then another user logs on and gets assigned to the same bus, at first the new user sees the GUI Main Page – but as soon as he accesses any port, he automatically enters Auto Scan Mode (since he is sharing the bus with the original user). Any user on the bus can halt Auto Scan Mode by recalling the GUI Main Page. When this occurs, Auto Scan Mode stops and all the other users on the bus are switched to the port that was being accessed when Auto Scan Mode stopped.
Panel Array Mode	◆ If a user has invoked Panel Array Mode (see page 216), and then another user logs on and gets assigned to the same bus at first user, the new user sees the GUI Main Page – but as soon as he accesses any port, he automatically enters Panel Array Mode (since he is sharing the bus with the original user). ◆ Panel Array Mode continues until the original user stops it. (Administrators can override Panel Array Mode, however.) ◆ Only the user who starts Panel Array Mode can use the Skip Mode (see page 214), function. ◆ Only the user who starts Panel Array Mode can switch ports. Other users automatically switch to the ports that the original user selects. However, if one of the other users does not have access rights to the port that the original user switches to, that user will not be able to view the port. ◆ Individual users can increase or decrease the number of panels they wish to view in Panel Array Mode; however, the picture quality may decrease as the number of panels increases.

Users and Buses

- The KN8164V / KN8132V / KN4164V support eight remote buses. The first, ninth, 17th, etc., users are all on the first bus; the second, 10th, 18th, etc., users are all on the second bus; the third, 11th, 19th etc., users are all on the third bus; the fourth, 12th, 20th, etc., users are all on the fourth bus; the fifth, 13th, 21st, etc., users are all on the fifth bus; the sixth, 14th, 22nd, etc., users are all on the sixth bus; the seventh, 15th, 23rd, etc., users are all on the sixth bus; the eighth, 16th, 24th, etc., users are all on the eighth bus.
- All KVM over IP switches support independent bus switching. With independent bus switching, if a user switches to a port that is being utilized by someone on a different bus, only the user that switched ports goes to the new port and the new bus – the other users on the original bus remain on the original port and original bus.

Note: 1. Independent bus switching does not work when Auto Scan Mode or Panel Array Mode is being used by one of the members of the bus.

2. If *Enable First Rider Transfer* is enabled (see page 156), only the first user on a bus can switch to an un-accessed port. Other users on the bus cannot switch ports unless there is a bus that is already connected to the port they would like to access, or there is a free bus available.

- We recommend that the user who starts Panel Array Mode set it to display at least four panels. Otherwise, it is possible that the other users may only receive part of the picture.

This Page Intentionally Left Blank

Chapter 13
The Log Server

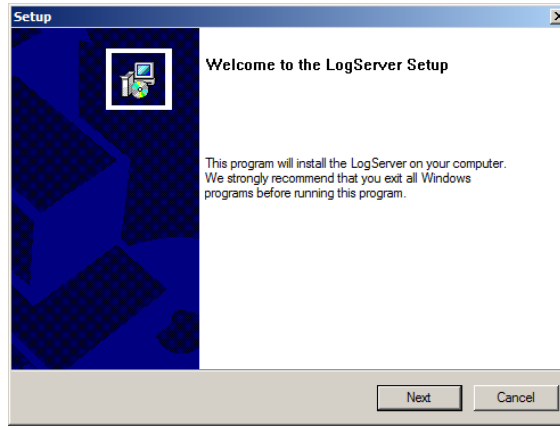
The Windows-based Log Server is an administrative utility that records all the events that take place on selected KVM over IP switches and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. Log into the KVM over IP switch (see page 43).
2. Click the *Download* tab and download the Log Server AP program.
3. Go to the location on your hard disk that you downloaded the Log Server program to, and double click its icon (*LogSetup.exe*) to bring up the Windows Client Connection Screen:

   Note: If the browser cannot run the file, save it to disk, instead, and run the file from your disk.

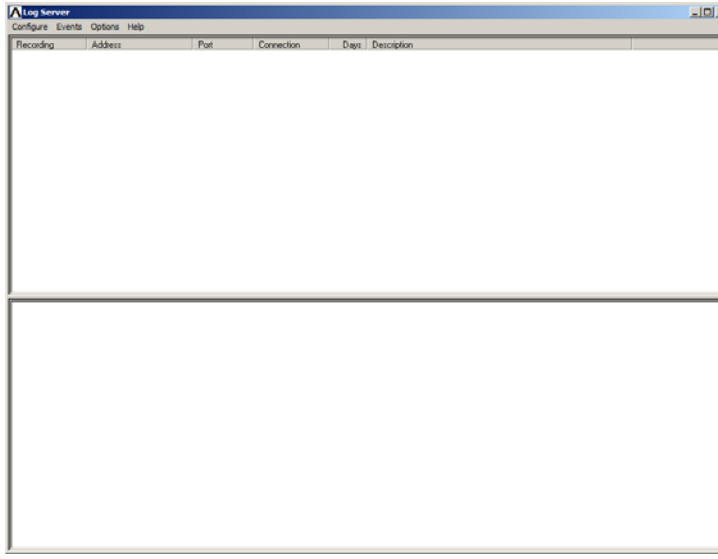
   The Log Server installation screen appears:


Setup
Welcome to the LogServer Setup
This program will install the LogServer on your computer.
We strongly recommend that you exit all Windows
programs before running this program.
Next
Cancel

4. Click **Next**. Then follow the on-screen instructions to complete the installation and have the Log Server program icon placed on your desktop.

Starting Up

To start the Log Server, either double click the program icon, or key in the full path to the program on the command line. The first time you run it, a screen similar to the one below appears:



Note: 1. The MAC address of the Log Server computer must be specified in the*ANMS* settings – see *Log Server*, page 163.

2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver. See *The Log Server program does not run.*, page 247 if the program doesn't start.

The screen is divided into three components:

- A *Menu Bar* at the top
- A panel that will contain a list of KVM over IP switches in the middle (see *The Log Server Main Screen*, page 227).
- A panel that will contain an *Events List* at the bottom

Each of the components is explained in the sections that follow.

The Menu Bar

The Menu bar consists of four items:

- Configure
- Events
- Options
- Help

These are discussed in the sections that follow.

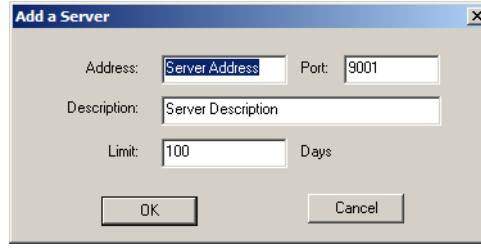
Note: If the Menu Bar appears to be disabled, click in the List window to enable it.

Configure

The Configure menu contains three items: Add; Edit; and Delete. They are used to add new units to the List; edit the information for units already on the list; or delete units from the list.

- To add a unit to the list, click **Add**.
- To edit or delete a listed unit, first select the target in the List window, then open this menu and click **Edit** or **Delete**.

When you choose *Add* or *Edit*, a dialog box, similar to the one below, appears:



A description of the fields is given in the table, below:

Field	Explanation
Address	This can either be the IP address of the computer the Log Server is running on, or its DNS name.
Port	The port number that was assigned to the Log Server under *Device Management* (see *Log Server*, page 163).
Description	This field is provided so that you can put in a descriptive reference for the unit to help identify it.
Limit	This specifies the number of days that an event should be kept in the Log Server's database. Events that exceed the amount of time specified here can be removed with the Maintenance function (see *Maintenance:*, page 225).

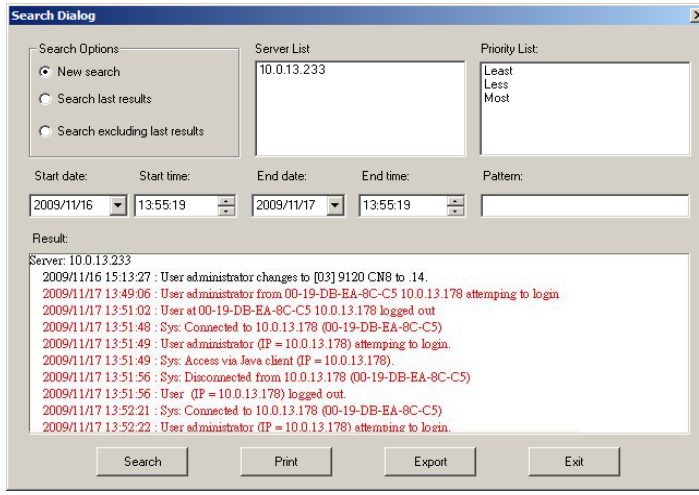
Fill in or modify the fields, then click **OK** to finish.

Events

The Events Menu has two items: *Search* and *Maintenance*.

Search:

Search allows you to search for events containing specific words or strings. When you access this function, a screen, similar to the one below, appears:



A description of the items is given in the table, below:

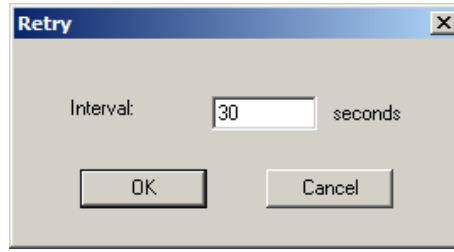
Item	Description
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected unit.
Search last results	This is a secondary search performed on the events that resulted from the previous search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected unit excluding the events that resulted from the previous search.
Server List	KVM over IP switches are listed according to their IP address. Select the unit that you want to perform the search on from this list. You can select more than one unit for the search. If no units are selected, the search is performed on all of them.
Priority	Sets the level for how detailed the search results display should be. *Least* is the most general; *Most* is the most specific. Least results appear in black; Less results appear in blue; Most results appear in red.
Start Date	Select the date that you want the search to start from. The format follows the YYYY/MM/DD convention, as follows: 2009/11/04
Start Time	Select the time that you want the search to start from. The format follows the HH:MM:SS convention.
End Date	Select the date that you want the search to end at.
End Time	Select the time that you want the search to end at.
Pattern	Key in the pattern that you are searching for here. The multiple character wildcard (%) is supported. E.g., h%ds would match hands and hoods.
Results	Lists the events that contained matches for the search.
Search	Click this button to start the search.
Print	Click this button to print the search results.
Export	Click this button to save the search results to file.
Exit	Click this button to exit the Log Server.

Maintenance:

This function allows the administrator to perform manual maintenance of the database, such as erasing specified records before their expiration time is up.

Options

Network Retry allows you to set the number of seconds that the Log Server should wait before attempting to connect if its previous attempt to connect failed. When you click this item, a dialog box, similar to the one below, appears:



Key in the number of seconds, then click **OK** to finish.

Help

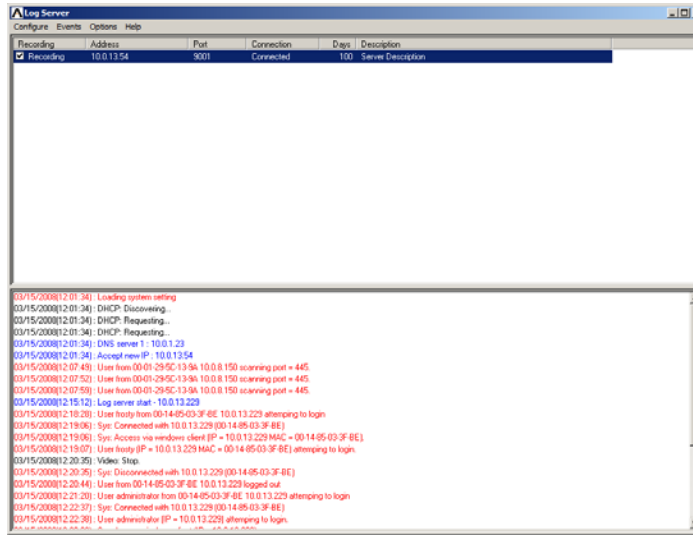
From the Help menu, click Contents to access the online Windows Help file. The help file contains instructions about how to setup, operation and troubleshoot the Log Server.

The Log Server Main Screen

Overview

The Log Server Main Screen is divided into two main panels.

- The upper (List) panel lists all of the units that have been selected for the Log Server to track (see *Configure*, page 223).
- The lower (Event) panel displays the tick information for the currently selected unit. (If there are more than one unit, the selected unit is the one that is highlighted).
- To select a unit in the list, simply click on it.


Log Server
Configure Events Options Help
Recording Address Port Connection Days Description
Recording 10.0.13.54 9001 Connected 100 Server Description
(03/15/2008[12:01:34]) : Loading system setting
(03/15/2008[12:01:34]) : DHCP: Discovering...
(03/15/2008[12:01:34]) : DHCP: Requesting...
(03/15/2008[12:01:34]) : DHCP: Requesting...
(03/15/2008[12:01:34]) : DNS server 1 : 10.0.1.23
(03/15/2008[12:01:34]) : Accept new IP : 10.0.13.54
(03/15/2008[12:07:49]) : User from 00-01-29-5C-13-9A 10.0.8.150 scanning port = 445.
(03/15/2008[12:07:52]) : User from 00-01-29-5C-13-9A 10.0.8.150 scanning port = 445.
(03/15/2008[12:07:59]) : User from 00-01-29-5C-13-9A 10.0.8.150 scanning port = 445.
(03/15/2008[12:15:12]) : Log server start - 10.0.13.229
(03/15/2008[12:18:28]) : User frosty from 00-14-85-03-3F-BE 10.0.13.229 attemping to login
(03/15/2008[12:19:06]) : Sys: Connected with 10.0.13.229 (00-14-85-03-3F-BE)
(03/15/2008[12:19:06]) : Sys: Access via windows client [IP = 10.0.13.229 MAC = 00-14-85-03-3F-BE]
(03/15/2008[12:19:07]) : User frosty (IP = 10.0.13.229 MAC = 00-14-85-03-3F-BE) attemping to login.
(03/15/2008[12:20:35]) : Video: Stop.
(03/15/2008[12:20:35]) : Sys: Disconnected with 10.0.13.229 (00-14-85-03-3F-BE)
(03/15/2008[12:20:44]) : User from 00-14-85-03-3F-BE 10.0.13.229 logged out
(03/15/2008[12:21:20]) : User administrator from (00-14-85-03-3F-BE 10.0.13.229 attemping to login
(03/15/2008[12:22:37]) : Sys: Connected with 10.0.13.229 (00-14-85-03-3F-BE)
(03/15/2008[12:22:38]) : User administrator [IP = 10.0.13.229] attemping to login.

The List Panel

The List panel contains six fields:

Field	Explanation
Recording	Determines whether the Log Server records the ticks for this unit, or not. If the Recording checkbox is checked, the field displays Recording, and the ticks are recorded. If the Recording checkbox is not checked, the field displays *Paused*, and the ticks are not recorded. **Note:** Even though a unit is not the currently selected one, if its Recording checkbox is checked, the Log Server will still record its ticks.
Address	This is the IP Address or DNS name that was given to the unit when it was added to the Log Server (see *Configure*, page 223).
Port	This is the Access Port number assigned to the unit (see *Configure*, page 223).
Connection	◆ If the Log Server is connected to the unit, this field displays *Connected*. ◆ If the Log Server is not connected, this field displays *Waiting*. This means that the Log Server's MAC address has not been set properly. It needs to be set on the *Device Management Date/Time* page (see page 184).
Days	This field displays the number of days that the unit's log events are to be kept in the Log Server's database before expiration (see *Configure*, page 223).
Description	This field displays the descriptive information given for the unit when it was added to the Log Server (see *Configure*, page 223).

The Event Panel

The lower panel displays log events for the currently selected unit. Note that if there are more than one units, even though they aren't currently selected, if their *Recording* checkbox is checked, the Log Server records their log events and keeps them in its database.

Appendix

Safety Instructions

General

- This product is for indoor use only.
- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- To prevent damage to your installation it is important that all devices are properly grounded.
- The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.

- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or un-interruptible power supply (UPS).
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.
- Additional protection to secure and fix the equipment is needed if the equipment is installed by stacking; by locking it to the rack, screwing it to the frame, or other similar methods.

- Keep the Cat 5e/6 cable as far away as possible from potential sources of EMI, such as electrical cables, transformers, and light fixtures. Do not tie the cables to electrical conduits or lay the cables on electrical fixtures.

Rack Mounting

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Make sure that all equipment used on the rack – including power strips and other electrical connectors – is properly grounded.
- Ensure that proper airflow is provided to devices in the rack.
- Ensure that the operating ambient temperature of the rack environment does not exceed the maximum ambient temperature specified for the equipment by the manufacturer
- Do not step on or stand on any device when servicing other devices in a rack.

Consignes de sécurité

Général

- Ce produit est destiné exclusivement à une utilisation à l'intérieur.
- Veuillez lire la totalité de ces instructions. Conservez-les afin de pouvoir vous y référer ultérieurement.
- Respectez l'ensemble des avertissements et instructions inscrits sur l'appareil.
- Ne placez jamais l'unité sur une surface instable (chariot, pied, table, etc.). Si l'unité venait à tomber, elle serait gravement endommagée.
- N'utilisez pas l'unité à proximité de l'eau.
- Ne placez pas l'unité à proximité de ou sur des radiateurs ou bouches de chaleur.
- Le boîtier de l'unité est doté de fentes et d'ouvertures destinées à assurer une ventilation adéquate. Pour garantir un fonctionnement fiable et protéger l'unité contre les surchauffes, ces ouvertures ne doivent jamais être bloquées ou couvertes.
- L'unité ne doit jamais être placée sur une surface molle (lit, canapé, tapis, etc.) car ses ouvertures de ventilation se trouveraient bloquées. De même, l'unité ne doit pas être placée dans un meuble fermé à moins qu'une ventilation adaptée ne soit assurée.
- Ne renversez jamais de liquides de quelque sorte que ce soit sur l'unité.
- Débranchez l'unité de la prise murale avant de la nettoyer. N'utilisez pas de produits de nettoyage liquide ou sous forme d'aérosol. Utilisez un chiffon humide pour le nettoyage de l'unité.
- L'appareil doit être alimenté par le type de source indiqué sur l'étiquette. Si vous n'êtes pas sûr du type d'alimentation disponible, consultez votre revendeur ou le fournisseur local d'électricité.
- Afin de ne pas endommager votre installation, vérifiez que tous les périphériques sont correctement mis à la terre.
- L'unité est équipée d'une fiche de terre à trois fils. Il s'agit d'une fonction de sécurité. Si vous ne parvenez pas à insérer la fiche dans la prise murale, contactez votre électricité afin qu'il remplace cette dernière qui doit être obsolète. N'essayez pas d'aller à l'encontre de l'objectif de la fiche de terre. Respectez toujours les codes de câblage en vigueur dans votre région/pays.

- L’équipement doit être installé à proximité de la prise murale et le dispositif de déconnexion (prise de courant femelle) doit être facile d’accès.
- La prise murale doit être installée à proximité de l’équipement et doit être facile d’accès.
- Veillez à ce que rien ne repose sur le cordon d’alimentation ou les câbles. Acheminez le cordon d’alimentation et les câbles de sorte que personne ne puisse marcher ou trébucher dessus.
- En cas d’utilisation d’une rallonge avec cette unité, assurez-vous que le total des ampérages de tous les produits utilisés sur cette rallonge ne dépasse pas l’ampérage nominal de cette dernière. Assurez-vous que le total des ampérages de tous les produits branchés sur la prise murale ne dépasse pas 15 ampères.
- Pour contribuer à protéger votre système contre les augmentations et diminutions soudaines et transitoires de puissance électrique, utilisez un parasurtenseur, un filtre de ligne ou un système d’alimentation sans coupure (UPS).
- Placez les câbles du système et les câbles d’alimentation avec précaution ; veillez à ce que rien ne repose sur aucun des câbles.
- Lors du branchement ou du débranchement à des blocs d’alimentation permettant la connexion à chaud, veuillez respecter les lignes directrices suivantes:
- Installez le bloc d’alimentation avant de brancher le câble d’alimentation à celui-ci.
- Débranchez le câble d’alimentation avant de retirer le bloc d'alimentation.
- Si le système présente plusieurs sources d’alimentation, déconnectez le système de l'alimentation en débranchant tous les câbles d'alimentation des blocs d'alimentation.
- N’insérez jamais d’objets de quelque sorte que ce soit dans ou à travers les fentes du boîtier. Ils pourraient entrer en contact avec des points de tension dangereuse ou court-circuiter des pièces, entraînant ainsi un risque d’incendie ou de choc électrique.
- N’essayez pas de réparer l’unité vous-même. Confiez toute opération de réparation à du personnel qualifié.
- Si les conditions suivantes se produisent, débranchez l’unité de la prise murale et amenez-la à un technicien qualifié pour la faire réparer:
  - Le cordon d’alimentation ou la fiche ont été endommagés ou éraillés.
  - Du liquide a été renversé dans l’unité.

- L’unité a été exposée à la pluie ou à l’eau.
- L’unité est tombée ou le boîtier a été endommagé.
- Les performances de l’unité sont visiblement altérées, ce qui indique la nécessité d’une réparation.
- L’unité ne fonctionne pas normalement bien que les instructions d’utilisation soient respectées.

- N’utilisez que les commandes qui sont abordées dans le mode d’emploi. Le réglage incorrect d’autres commandes peut être à l’origine de dommages qui nécessiteront beaucoup de travail pour qu’un technicien qualifié puisse réparer l’unité.
- Tenez le câble de catégorie 5e/6 le plus éloigné possible des sources potentielles d’interférences électromagnétiques, telles que les câbles électriques, transformateurs et appareils d’éclairage. Ne nouez pas les câbles à des conduits électriques et ne les faites pas passer sur des installations électriques.

Montage sur bâti

- Avant de travailler sur le bâti, assurez-vous que les stabilisateurs sont bien fixées sur le bâti, qu'ils sont étendus au sol et que tout le poids du bâti repose sur le sol. Installez les stabilisateurs avant et latéraux sur un même bâti ou bien les stabilisateurs avant si plusieurs bâtis sont réunis, avant de travailler sur le bâti.
- Chargez toujours le bâti de bas en haut et chargez l'élément le plus lourd en premier.
- Assurez-vous que le bâti est à niveau et qu'il est stable avant de sortir une unité du bâti.
- Agissez avec précaution lorsque vous appuyez sur les loquets de libération du rail d'unité et lorsque vous faites coulisser une unité dans et hors d'un bâti ; vous pourriez vous pincer les doigts dans les rails.
- Une fois qu'une unité a été insérée dans le bâti, étendez avec précaution le rail dans une position de verrouillage puis faites glisser l'unité dans le bâti.
- Ne surchargez pas le circuit de l'alimentation CA qui alimente le bâti. La charge totale du bâti ne doit pas dépasser 80 % de la capacité du circuit.
- Assurez-vous que tous les équipements utilisés sur le bâti, y-compris les multiprises et autres connecteurs électriques, sont correctement mis à la terre.
- Assurez-vous que les unités présentes dans le bâti bénéficie d'une circulation d'air suffisante.
- Assurez-vous que la température ambiante de fonctionnement de l'environnement du bâti ne dépasse pas la température ambiante maximale spécifiée pour l'équipement par le fabricant.
- Ne marchez sur aucun appareil lors de la maintenance d'autres appareils d'un bâti.

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **http://eservice.aten.com**
- For telephone support, see *Telephone Support*, page iv

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://www.aten-usa.com/support
Telephone Support		1-888-999-ATEN ext 4988

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

Specifications

KN4164V / KN8132V / KN8164V

Function			KN4164V	KN8132V	KN8164V
Computer Connections	Direct		64	32	64
	Max		512		
Port Selection			Pushbutton / GUI / Hotkey		
Connectors	Console Port	Keyboard	1 x USB Type A Female (Black)		
		Video	1 x DVI-D Female (White) 1 x HDB-15 (Blue)		
		Mouse	1 x USB Type A Female (Black)		
		Audio	2 x Audio Jack (Female)		
		LUC Port	1 x Mini-USB Female (Black)		
		Console Ext.	1 x RJ-45 Female (Black)		
	KVM Port		64 x RJ-45 Female (Black)	32 x RJ-45 Female (Black)	64 x RJ-45 Female (Black)
	Power		2 x 3-prong AC socket		
	LAN		2 x RJ-45 Female (Black)		
	PON		1 x RJ-45 Female (Black)		
	Modem		1 x RJ-45 Female (Black)		
	USB (Console/Virtual Media)		3 x USB Type A Female (Black)		
Switches	Reset		1 x Semi-recessed Pushbutton		
	Power		2 x Rocker Switch		
	Port Selection		2 x Pushbutton		
LEDs	On Line		64 (Green)	32 (Green)	64 (Green)
	Selected		64 (Orange)	32 (Orange)	64 (Orange)
	Power		2 (Blue)		
	Link 10/100/1000 Mbps		2 (Orange / Green)		
Emulation	Keyboard / Mouse		PS/2 / USB (PC, Mac, Sun) / Serial		
Video			1920 x 1200 @ 60Hz		
Scan Interval			1–255 secs		
I/P Rating			100–240VAC; 50–60Hz; 1.0A	100–240VAC; 50–60Hz; 1.0A	100–240VAC; 50–60Hz; 1.0A

Function		KN4164V	KN8132V	KN8164V
Power Consumption	Single Power	110V/67.9W; 220V/ 66.4W	110V/72.6W; 220V/ 71.7W	110V/82.5W; 220V/ 81W
	Dual Power	110V/26.2W; 220V/ 25.4W	110V/28.3W; 220V/ 28W	110V/35.5W; 220V/ 34W
Environment	Operating Temp.	0–40° C		
	Storage Temp.	-20–60° C		
	Humidity	0–80% RH		
Physical Properties	Housing	Metal; Non-condensing		
	Weight	7.00 kg	5.80 kg	7.07 kg
	Dimensions L x W x H	43.36 x 41.26 x 8.80 cm	43.36 x 41.21 x 4.40 cm	43.36 x 41.26 x 8.80 cm

Troubleshooting

General Operation

Problem	Resolution
I am confused about which equipment the terms *Local* and *Remote* refer to.	See *Terminology*, page xvii for details
Erratic Operation	The KVM over IP switch needs to be started before any cascaded switches. 1. Make sure to power it on before powering on the switch. 2. If the cascaded switch was started before the KVM over IP switch, reset or restart the cascaded switch.
	Press and release the *Reset* switch (see *Reset Switch*, page 11).
I have been given an account but I am unable to log in.	1. Make sure that you have correctly specified your Username and Password. 2. Make sure that the administrator has given you the necessary permission to access the switch. 3. Ask your administrator to see if the switch is under CC management. If it is, he will have to resolve the situation either by disabling CC management on the switch (see page 162), or by deselecting it on the CC server (see the CC User Manual for details).
I can't access the switch, even though I have specified the IP address and port number correctly.	If the switch is behind a router, the router's *Port Forwarding* (also referred to as *Virtual Server*) feature must be configured. See *Port Forwarding*, page 254, for details.
When logging in from a browser, the following message appears: *404 Object Not Found.*	If a login string has been set, make sure to include the forward slash and correct login string when you specify the KVM over IP switch's IP address. (See *Login String*, page 177.)
Sudden loss of network connection.	Close your connection to the KVM over IP switch. Wait approximately 30 seconds, and log in again.
No remote server video display on the client computer.	Check that your KVM Adapter Cable's firmware version is the same as the version stored in the switch's Main firmware. See *Upgrade Adapters*, page 198 for details
	Set the remote server resolution to 1280 x 1024 or less.

Problem	Resolution
No remote server video display on the client computer, but mouse movements appear on the local console and mouse clicks have no effect	Press and release the left Alt key, then press and release the right Alt key
The display on the client computer is distorted and performing an Autosync doesn't resolve the problem.	Switch ports to a port with a different resolution, then switch back. If the above didn't resolve the problem, change the resolution and refresh rate for the system running on the port. Afterward, you can either run at the new resolution, or switch back to the original resolution.
The Lock Key LEDs on the Control Panel don't accurately reflect the actual locked status of my keyboard input.	When you first connect, the LED display may not accurately reflect the LEDs on your keyboard. To resolve the problem, click the LEDs on the Control Panel until they match your keyboard. Afterward, when you change them from the keyboard they will change on the Control Panel.
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See *Trusted Certificates*, page 268, for details.
In multiuser operation I had exclusive (or occupy) rights on the port I was viewing. After I recalled the Port Access page and then came back to the port I was occupying, it had been taken over by another user. Why did this happen?	If you try to return to the port by selecting again in the tree, the switch acts as if you are accessing the port for the first time. If another user was waiting on the port, he takes precedence and gets the port. The correct way to return to the port is to click the *Close* icon at the top right of the Port Access page.

Mouse Problems

Problem	Resolution
Mouse and/or Keyboard not responding.	Check that your KVM Adapter Cable's firmware version is the same as the version stored in the switch's Main firmware. See *Upgrade Adapters*, page 198 for details
	Unplug the cable(s) from the console port(s), then plug it/ them back in.
Mouse movement extremely slow	There is too much data being transferred for your connection to keep up with. Lower the video quality (see *Video Settings*, page 73) so that less video data is transmitted.
There are two mouse pointers after the remote server is accessed.	You can select another pointer type. See *Mouse Pointer Type*, page 86 for details
When the mouse pointer is in Single Pointer mode, I can't access the Control Panel.	Recall the Control Panel and immediately change the pointer to Dual mode.
Why is there a Dual Pointer mode?	When you are not in Mouse DynaSync Mode, you need the two pointers so that you know the remote server pointer is actually at the location you think it is at. Otherwise, you might perform a mouse operation and because of net lag the remote server pointer may not be at the location that your client computer pointer is at.
Mouse pointer confusion	If you find the display of two mouse pointers (local and remote) to be confusing or annoying, you can use the *Toggle Mouse Display* function to shrink the non-functioning pointer. See *Toggle mouse display,* page 65, and *Mouse Pointer Type*, page 86.
When I log in with my Windows system, the local and remote mouse pointers do not sync.	1. Check the status of the *Mouse Sync Mode* setting (see *Mouse DynaSync Mode*, page 88). If it is set to *Automatic*, change the setting to *Manual* and refer to the information for *Manual Mouse Synchronization* on page 89. 2. If you are in Manual mode, use the *AutoSync* feature (see *Video Settings*, page 73), to sync the local and remote monitors. 3. If that doesn't resolve the problem, use the *Adjust Mouse* feature (see *Adjust mouse*, page 65) to bring the pointers back in step. 4. If the above fails to resolve the problem, refer to *Additional Mouse Synchronization Procedures*, page 265, for further steps to take.

Problem	Resolution
When I log in with my Mac system, the local and remote mouse pointers do not sync.	There are two automatic Mouse DynaSync settings: the default, and Mac2. If mouse synchronization is not satisfactory with the default, try the Mac 2 setting. See the Note on page 89 for details.
When I log in with my Sun system, the local and remote mouse pointers do not sync	Automatic Mouse DynaSync sync only supports USB mice on Windows and Mac (G4 or higher) systems. You must sync the pointers manually. See *Mouse DynaSync Mode*, page 88, and *Manual Mouse Synchronization*, page 89, for further details. After doing the above, refer to *Sun / Linux*, page 266, under *Additional Mouse Synchronization Procedures* for further steps to take.
When I log in with my Linux system, the local and remote mouse pointers do not sync.	Automatic Mouse DynaSync sync only supports USB mice on Windows and Mac (G4 or higher) systems. You must sync the pointers manually. See *Mouse DynaSync Mode*, page 88, *Manual Mouse Synchronization*, page 89, and *Mac and Linux Considerations*, page 89, for further details. After doing the above, refer to *Sun / Linux*, page 266, (under *Additional Mouse Synchronization Procedures*), for further steps to take.

Virtual Media

Problem	Resolution
Virtual Media doesn't work.	The remote server's mainboard does not support USB. If there is a newer firmware and BIOS version for the remote server's mainboard – one that supports USB – get it from the manufacturer and upgrade the server's mainboard firmware and BIOS.
There is no Virtual Media icon on my Control Panel.	1. Virtual Media only supports devices connected with KA7166, KA7168, KA7169, KA7175, KA7176 or KA7177 KVM Adapter Cables with V-Series KVM over IP switches. 2. You must be have Administrator privileges on your client computer. (This is a Windows limitation.)
I can't boot my remote server from my Virtual Media drive.	Your remote server's BIOS doesn't support booting from a USB drive. Get the latest firmware and BIOS version for your mainboard from the manufacturer and upgrade your mainboard BIOS.
If I connect a USB floppy drive to a remote server, it can boot the remote server. But, if I map it to the remote server as a Virtual Media drive, it cannot boot the remote server.	USB floppy drives have two types of format: UFI and CBI. Both can be used for OS level virtual media functions, but currently only UFI is supported for BIOS level (such as boot) functions.
I cannot mount a Folder as a Virtual Media device.	If the actual Folder is formatted with the FAT16 file system, it cannot be mounted if its size exceeds 2GB.

Web Browser

Problem	Resolution
After upgrading the firmware, after logging in with my web browser, the switch appears to still be using the old firmware version.	The switch is using the new firmware version but the browser is displaying a page that is stored in its cache. Simply log out and clear your browser's cache. ◆ **IE:** Tools → Internet Options → Temporary Internet Files → Delete Files ◆ **Firefox:** Tools → Clear Private Data
Firefox only opens the Java Client Viewer. It doesn't open the WinClient ActiveX Viewer.	The WinClient ActiveX Viewer requires ActiveX. Since Firefox doesn't support ActiveX only the Java Client Viewer is available.

The WinClient ActiveX Viewer and the WinClient AP

Problem	Resolution
My KVM over IP units don't show up in the *Server List* window when I start the WinClient AP program.	Only units whose Access Port settings for *Program* (see page 157) match the number specified for *Port* in the Server area of this dialog box appear in the Server List window. Make sure that your entry for Port matches the entry you have specified for Program on the Device Management *Network* page.
The WinClient ActiveX Viewer and the WinClient AP won't connect to the KVM over IP switch.	DirectX 8.0 or higher must be installed on your client computer.
After upgrading the firmware, the WinClient ActiveX Viewer or WinClient AP do not run.	The old version of your *.ocx* file was not deleted. You must delete the old file. There are two methods to delete the file. 1. For the ActiveX Viewer: Open IE → Tools → Manage Add-ons. Delete or disable all occurrences of WinClient. 2. For the WinClient AP: Open Explorer and search for WinClient.ocx. Delete all occurrences.
Part of the remote window is off my monitor.	1. Perform an Auto Sync (see *WinClient Control Panel Functions*, page 61 for details). 2. If *Keep Screen Size* is not enabled (see *Screen Options*, page 91), use the *AutoSync* feature (see *Video Settings*, page 73), to sync the local and remote monitors. 3. If *Keep Screen Size* is enabled, you can scroll to the areas that are off screen.
The remote screen is rotated 90 degrees.	Enable *Keep Screen Size* (see *Control Panel Configuration*, page 90).
I cannot run *Net Meeting* when the WinClient is running.	Enable *Keep Screen Size* (see *Control Panel Configuration*, page 90).
After logging in I can't open the WinClient ActiveX viewer.	1. You don't have the authority to install the *WinClient Control* add-on on your client computer. Have the person with administrator privileges on your client computer run the program the first time to get it installed. It will open for you after that. 2. Under Vista, you must also add the switch's URL address to the list of trusted sites: Tools → Internet Options → Security → Trusted Sites → Sites.

Problem	Resolution
Under Vista, after I open the WinClient ActiveX viewer and try to mount a driver or removable disk, I get a “Driver not ready” message.	This is a result of Vista’s UAC (User Account Control). There are two methods to resolve this problem: 1. If you are your client computer’s administrator, open your browser by right clicking its icon and choosing **Run as...** then choose to run the browser with the administrator account. 2. If you are not your client computer’s administrator, you must ask your client computer’s administrator to disable UAC.

The Java Applet and Java Client AP

Problem	Resolution
I can't connect to the KVM over IP switch.	1. The latest Java version must be installed on your client computer. 2. Check if you need to specify the Program port along with the IP address. See *Java Client AP Login*, page 49 for details 3. Close Java reopen it, and try again.
I have installed the latest Java JRE, but I am having performance and stability problems.	There may be issues with the latest version because it is so new. Try using a Java version that is one or two versions earlier than the latest one.
After upgrading the firmware, after logging in with the Java Client Viewer or the Java Client AP, the switch appears to still be using the old firmware version.	Log out. Delete your Java temporary internet files as follows: 1. Open Control Panel → Java. 2. In the *Temporary Internet Files* section, click **Settings**. 3. In the *Disk Space* section, click **Delete Files**. 4. In the dialog box that comes up, click **OK**.
The national language characters that I input do not appear.	Change the keyboard language of your client computer to English-UK. Use the KVM over IP switch’s *On-Screen Keyboard* and set the on-screen keyboard to the same language that the other system is using. (See *The On-Screen Keyboard*, page 84.)
Java performance deteriorates.	Exit the program and start again.
Pressing the Windows Menu key has no effect.	Java doesn't support the Windows Menu key.
When I try to **Add** a folder to be mounted as a virtual media drive, I can’t select the folder. My only choice is *Desktop*.	In the folder selection entry field, enter the root directory of the folder you want to add. After that, the folders contained under the root directory will display. You can now navigate to the folder you want to select.

Sun Systems

Problem	Resolution
Video display problems with HDB15 interface systems (e.g. Sun Blade 1000 servers).*	The display resolution should be set to 1024 x 768 @ 60Hz: **Under Text Mode:** Go to OK mode and issue the following commands: setenv output-device screen:r1024x768x60 reset-all **Under XWindow:** 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out 3. Log in
Video display problems with 13W3 interface systems (e.g. Sun Ultra servers).*	The display resolution should be set to 1024 x 768 @ 60Hz: **Under Text Mode:** Go to OK mode and issue the following commands: setenv output-device screen:r1024x768x60 reset-all **Under XWindow:** 1. Open a console and issue the following command: fbconfig -res 1024x768x60 2. Log out 3. Log in

***** These solutions work for most common Sun VGA cards. If using them fails to resolve the problem, consult the Sun VGA card's manual.

Mac Systems

Problem	Resolution
When I log in to the KVM over IP switch with my Safari browser, it hangs when I use the Snapshot feature.	Force close Safari, then reopen it. Don't use the Snapshot feature in the future.
	To use the Snapshot feature with Safari, upgrade to Mac OS 10.4.11 and Safari 3.0.4.

Redhat Systems

Problem	Resolution
With Redhat 9.0 (2.4.20-8) installed as a server, the keyboard and mouse aren't working normally with the KA7175/KA7176 console modules.	Choose the AS3.0 setting for your mouse synchronization mode. See *Mac and Linux Considerations*, page 89 for details
With Redhat 9.0 (2.4.20-8) installed as a desktop system, the keyboard and mouse aren't working normally with the KA7175/KA7176 console modules.	First, plug your keyboard and mouse into a USB 2.0 hub, then plug the hub into the Redhat 9.0 server.

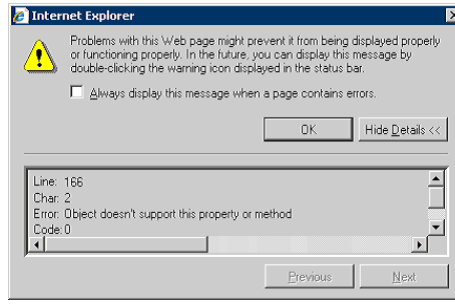
The Log Server

Problem	Resolution
The Log Server program does not run.	The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database. This driver is automatically installed with Windows ME, 2000 and XP. For Windows 98 or NT, you will have to go to the Microsoft download site: http://www.microsoft.com and do a search for *MDAC* to retrieve the driver file: MDAC 2.7 RTM Refresh (2.70.9001.0) Since this driver is used in Windows Office Suite, an alternate method of obtaining it is to install Windows Office Suite. Once the driver file or Suite has been installed, the Log Server will run.

Panel Array Mode

Problem	Resolution
Low resolution video – the screens don't display clearly.	This sometimes occurs due to the screens being scaled to fit in the panels. Decrease the number of panels that are displayed.
When multiple remote users are logged in, some of them only receive a partial image.	The first user to invoke Panel Array Mode should set it to display at least four panels.
When I try to move forward or backward one port, the display sometimes moves forward two ports or remains on the original port.	This occurs occasionally due to a net lag problem. The array automatically moves through the ports at a pre-selected time. By the time it gets your input It has already moved forward a port on its own - but that hasn't shown up on your display as yet. So, when it moves ahead or back due to your input it appears to have moved two ports (from its own movement plus your "forward one port" command), or remains on the original port (from its own forward movement plus your "back one port" command).

Q1: When I open a viewer, the web page does not display or work correctly, and I receive an error message that is similar one of the following:


Internet Explorer
Problems with this Web page might prevent it from being displayed properly or functioning properly. In the future, you can display this message by double-clicking the warning icon displayed in the status bar.
Always display this message when a page contains errors.
OK
Hide Details <<
Line: 166
Char: 2
Error: Object doesn't support this property or method
Code: 0
Previous
Next

1. Reset the Internet Explorer security settings to enable Active Scripting, ActiveX controls, and Java applets

   By default, Internet Explorer 6 and some versions of Internet Explorer 5.x use the High security level for the Restricted sites zone and Microsoft Windows Server 2003 uses the High security level for both the Restricted sites zone and the Internet zone. To enable Active Scripting, ActiveX controls, and Java applets, follow these steps:

   a) Start Internet Explorer.

   b) On the Tools menu, click Internet Options.

   c) In the Internet Options dialog box, click Security.

   d) Click Default Level.

   e) Click OK.

2. Verify that Active Scripting, ActiveX, and Java are not blocked

   If some client computers work but others do not, verify that Internet Explorer or another program on your client computer such as an anti-virus program or a firewall are not configured to block scripts, ActiveX controls, or Java applets.

3. Verify that your anti-virus program is not set to scan the Temporary Internet Files or Downloaded Program Files folders

4. Delete all the temporary Internet-related files

   To remove all the temporary Internet related files from your client computer, follow these steps:

   a) Start Internet Explorer.

   b) On the Tools menu, click **Internet Options**.

   c) Click the *General* tab.

   d) Under Temporary Internet files, click **Settings**.

   e) Click **Delete Files**.

   f) Click **OK**.

   g) Click **Delete Cookies**.

   h) Click **OK**.

   i) Under History, click **Clear History**, and then click **Yes**.

   j) Click **OK**.

5. Make sure that you have the latest version of Microsoft DirectX installed

   For information about how to install the latest version of Microsoft DirectX, visit the following Microsoft Web site:

   http://www.microsoft.com/windows/directx/default.aspx?url=/windows/directx/downloads/default.htm

6. Make sure that you have the latest version of the Java JRE installed.

   For information about how to install the latest version of the JRE visit the Java Web site: www.java.com.

IP Address Determination

If you are an administrator logging in for the first time, you need to access the KVM over IP switch in order to give it an IP address that users can connect to. There are three methods to choose from. In each case, your client computer must be on the same network segment as the KVM over IP switch. After you have connected and logged in you can give the KVM over IP switch its fixed network address. (See *Network*, page 157.)

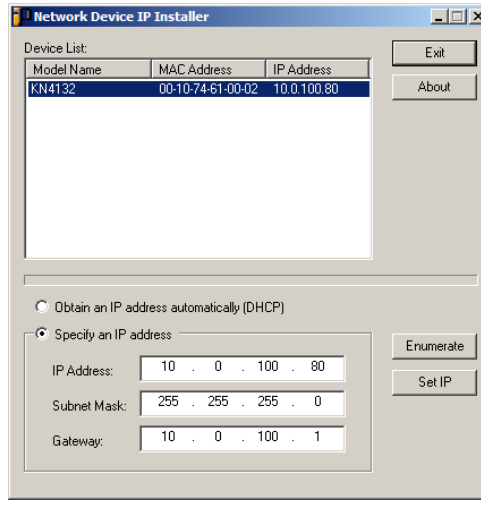
The Local Console

The easiest way to assign an IP address is from the local console. Refer to *First Time Setup*, page 37, for details on the procedure involved.

IP Installer

For client computers running Windows, an IP address can be assigned with the *IP Installer* utility. The utility can be obtained from the *Download* area of our website. Look under *Driver/SW*, and the model of your switch. After downloading the utility to your client computer, do the following:

1. Unzip the contents of *IPInstaller.zip* to a directory on your hard drive.
2. Go to the directory that you unzipped the IPInstaller program to and run *IPInstaller.exe*. A dialog box similar to the one below appears:



3. Select the KVM over IP switch in the *Device List*.

Note: 1. If the list is empty, or your device doesn't appear, click **Enumerate** to refresh the Device List.

2. If there is more than one device in the list, use the MAC address to pick the one you want. The KVM over IP switch's MAC address is located on its bottom panel.

4. Select either *Obtain an IP address automatically (DHCP)*, or *Specify an IP address*. If you chose the latter, fill the IP Address, Subnet Mask, and Gateway fields with the information appropriate to your network.
5. Click **Set IP**.
6. After the IP address shows up in the Device List, click **Exit**. See *IP Installer*, page 158 for more information.

Browser

1. Set your client computer's IP address to 192.168.0.*XXX*

   Where *XXX* represents any number or numbers except 60. (192.168.0.60 is the default address of the KVM over IP switch.)
2. Specify the switch's default IP address (192.168.0.60) in your browser, and you will be able to connect.
3. Assign a fixed IP address for the KVM over IP switch that is suitable for the network segment that it resides on.
4. After you log out, reset your client computer's IP address to its original value.

IPv6

At present, the KVM over IP switch supports three IPv6 address protocols: *Link Local IPv6 Address*, *IPv6 Stateless Autoconfiguration*, and *Stateful Autoconfiguration (DHCPv6)*.

Link Local IPv6 Address

At power on, the KVM over IP switch is automatically configured with a Link Local IPv6 Address (for example, fe80::210:74ff:fe61:1ef). To find out what the Link Local IPv6 Address is, log in with the KVM over IP switch's IPv4 address and open the *Device Management* → *Device Information* page. The address is displayed in the *General* list box (see page 154).

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

```
http://[fe80::2001:74ff:fe6e:59%5]
```

for the URL bar.

If you are logging in with the AP program, you would key:

```
fe80::2001:74ff:fe6e:59%5
```

for the *IP* field of the *Server* panel (see *Windows Client AP Login*, page 45).

Note: 1. To log in with the Link Local IPv6 Address, the client computer must be on the same local network segment as the KVM over IP switch

2. The %5 is the %interface used by the client computer. To see your client computer's IPv6 address: from the command line issue the following command: `ipconfig /all`. The % value appears at the end of the IPv6 address.

IPv6 Stateless Autoconfiguration

If the KVM over IP switch's network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the KVM over IP switch can obtain its prefix information from that device in order to generate its IPv6 address. For example, 2001::74ff:fe6e:59.

As above, the address is displayed in the *General* list box of the *Device Management* → *Device Information* page (see page 154).

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

```
http://[2001::74ff:fe6e:59]
```

for the URL bar.

If you are logging in with the AP program, you would key:

```
2001::74ff:fe6e:59
```

for the *IP* field of the *Server* panel (see *Windows Client AP Login*, page 45).

Port Forwarding

For devices located behind a router, port forwarding allows the router to pass data coming in over a specific port to a specific device. By setting the port forwarding parameters, you tell the router which device to send the data that comes in over a particular port to.

For example, if the KVM over IP switch connected to a particular router has an IP address of 192.168.1.180, you would log into your router's setup program and access the Port Forwarding (sometimes referred to as *Virtual Server*) configuration page. You would then specify 192.168.1.180 for the IP address and the port number you want opened for it (9000 for Internet access, for example).

Since configuration setup can vary somewhat for each brand of router, refer to the router's User Manual for specific information on configuring port forwarding for it.

Keyboard Emulation

Mac Keyboard

The PC compatible (101/104 key) keyboard can emulate the functions of the Mac keyboard. The emulation mappings are listed in the table below.

PC Keyboard	Mac Keyboard
[Shift]	Shift
[Ctrl]	Ctrl
[Ctrl] [1]	
[Ctrl] [2]	
[Ctrl] [3]	
[Ctrl] [4]	
[Alt]	Alt
[Print Screen]	F13
[Scroll Lock]	F14
	=
[Enter]	Return
[Backspace]	Delete
[Insert]	Help
[Ctrl]	F15

Note: When using key combinations, press and release the first key (Ctrl), then press and release the activation key.

Sun Keyboard

The PC compatible (101/104 key) keyboard can emulate the functions of the Sun keyboard when the Control key [Ctrl] is used in conjunction with other keys. The corresponding functions are shown in the table below.

PC Keyboard	Sun Keyboard
[Ctrl] [T]	Stop
[Ctrl] [F2]	Again
[Ctrl] [F3]	Props
[Ctrl] [F4]	Undo
[Ctrl] [F5]	Front
[Ctrl] [F6]	Copy
[Ctrl] [F7]	Open
[Ctrl] [F8]	Paste
[Ctrl] [F9]	Find
[Ctrl] [F10]	Cut
[Ctrl] [1]	
[Ctrl] [2]	
[Ctrl] [3]	
[Ctrl] [4]	
[Ctrl] [H]	Help
	Compose
	Meta

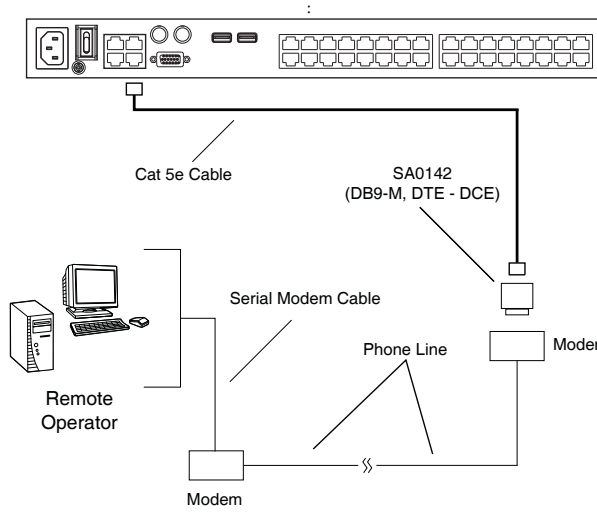
Note: When using key combinations, press and release the first key (Ctrl), then press and release the activation key.

PPP Modem Operation

Basic Setup

The KVM over IP switch can be accessed through its RS-232 port using a PPP dial-in connection, as follows:

1. Set up your hardware configuration to match the diagram, below:



2. From your client computer, use your modem dial-in program to dial into the KVM over IP switch's modem.

Note: 1. If you don't know the KVM over IP switch modem's serial parameters, get them from the KVM over IP administrator.
2. An example of setting up a modem dial-in program under Windows XP is provided on the next page.

3. Once the connection is established, open your browser, and specify **192.168.192.1** in the URL box.

Note: 1. The default username and password are blank.
2. For the modem session, the KVM over IP switch has an IP address of 192.168.192.1; the user side has an IP address of 192.168.192.101.

From here, operation is the same as if you had logged in from a browser or with the AP programs.

Connection Setup Example (Windows XP)

To set up a dial-in connection to the KVM over IP switch under Windows XP, do the following:

1. From the *Start* menu, select Control Panel → Network Connections → Create a New Connection.
2. When the *Welcome to the New Connection Wizard* dialog box appears, click **Next** to move on.
3. In the *Network Connection Type* dialog box, select *Connect to the network at my workplace*, then click **Next**.
4. In the *Network Connection* dialog box, select *Dial-up connection*, then click **Next**.
5. In the *Connection Name* dialog box, key in a name for the connection (for example, TPE-KN8132-01), then click **Next**.
6. In the *Connection Availability* dialog box, you can select either *Anyone's use* or *My use only*, depending on your preferences, then click **Next**.

   Note: If you are the only user on this client computer, this dialog box won't appear.

7. In the *Phone Number to dial* dialog box, key in the phone number of the modem connected to the KVM over IP switch (be sure to include country and area codes, if necessary), then click **Next**.
8. In the *Completing the New Connection Wizard* dialog box, check **Add a shortcut to this connection on my desktop**, then click **Finish**.

This completes the connection setup. Double click the desktop shortcut icon to make a PPP connection to the KVM over IP switch.

KA7140 Configuration and Operation

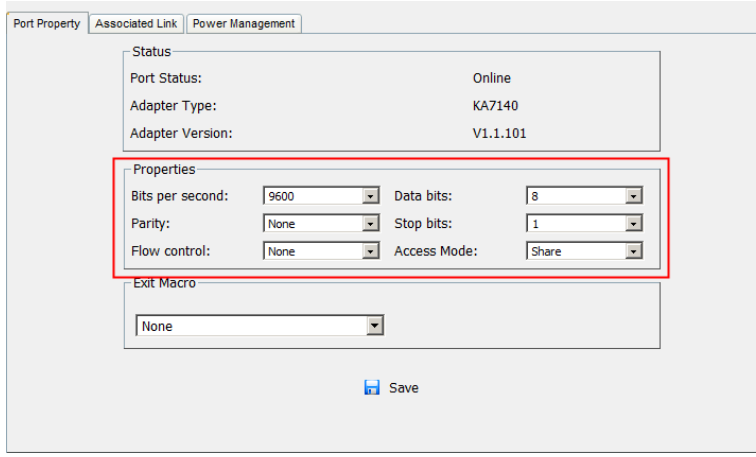
The KA7140 Adapter Cable connects a serial device to the KVM over IP switch.

Configuration

To configure the KA7140 to interact with the connected device, you need to set its serial parameters to match the parameters of the device, as follows:

1. In the Port Access page Sidebar, select the port that the KA7140 is connected to.
2. Select **Port Configuration** on the menu bar.

   The page comes up with the *Port Properties* tab selected:



3. In the *Properties* section, drop down each of the lists to select the port property values that match the ones used by the connected serial console device. The port property settings that the KA7140 supports are given in the following table:

Setting	Meaning
Bits per second (Baud Rate)	This sets the port's data transfer speed. Choices are from 300—38400 (drop down the list to see them all). Set this to match the baud rate setting of the serial console device. Default is 9600 (which is a basic setting for many serial console devices).
Data Bits	This sets the number of bits used to transmit one character of data. Choices are: 7 and 8. Set this to match the data bit setting of the serial console device. Default is 8 (which is the default for the majority of serial console devices).
Parity	This bit checks the integrity of the transmitted data. Choices are: None; Odd; Even. Set this to match the parity setting of the serial console device. Default is Odd.
Stop Bits	This indicates that a character has been transmitted. Set this to match the stop bit setting of the serial console device. Choices are: 1 and 2. Default is 1 (which is the default for the majority of serial console devices).
Flow Control	This allows you to choose how the data flow will be controlled. Choices are: None, Hardware, and XON/XOFF. Set this to match the flow control setting of the serial console device. Default is None. **Note:** *None* is only supported for baud rates of 9600 and lower. For baud rates greater than 9600, you must choose *Hardware* or *XON/XOFF*.
Access Mode	This allows you to set the serial console device's access mode. Choices are: Share, Occupy, and Exclusive. Default is Share. See *Access Mode*, page 128 for information regarding this function.

4. When you have finished making your selections, click **Save**.

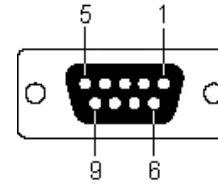
Operation

To operate the device connected to the port, in the Port Access page double click the port to establish a serial connection to the device.

KA7140 Pin Assignments

Pin assignments for the KA7140 Adapter are given in the table, below:

Pin	Assignment
1	DCD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	N/A

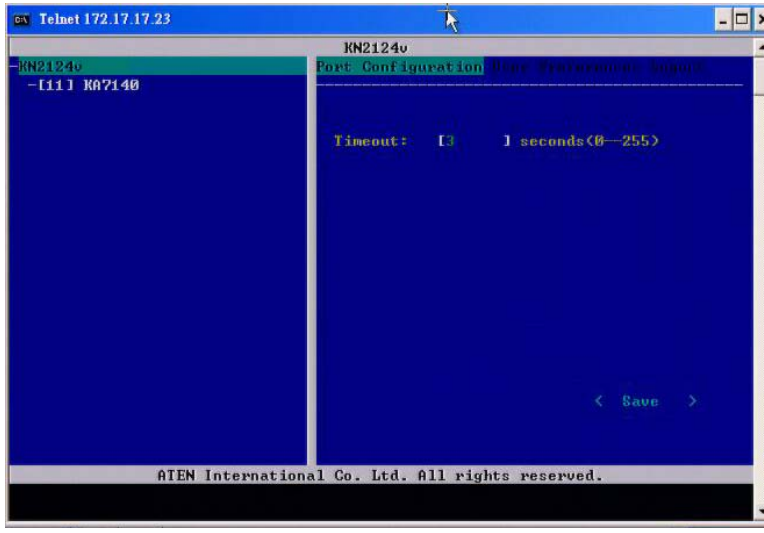


DB9 Female

Internal Serial Interface Configuration

The KVM over IP switch provides a function that lets you configure an attached device's serial interface parameters from within any accessed server. To do so:

1. From the accessed server, open a command line (terminal) session or third party serial application such as HypterTerminal or PuTTY.
2. Telnet or SSH to the KVM over IP switch's IP address.
3. Log in with your usual Username and Password to bring up the access screen:



Navigation

The left panel shows the KVM over IP switch at the top, and all the serial interface devices connected to it listed below. The right panel shows the configuration parameters at the top, with the configuration settings in the area below.

- Use the Left and Right Arrow keys (← and →) to move the highlight bar between the right and left panels, and to select the parameter to configure.
- Use the Up and Down Arrow Keys (↑ and ↓) to select among the switch and the serial devices in the left panel; use them to select the configuration items in the right panel.

Operation

- Use the Up and Down Arrow Keys (↑ and ↓) to highlight a device in the left panel, then press [Enter] to open a command line (terminal) session on the accessed device.
- When you have finished with your session, press the hotkey (see page 263 and 264) that brings you back to the access page.
- To finish with this function, move the highlight bar to *Logout* in the right panel of the access page; Press the Down Arrow key to highlight *Exit*, then press **[Enter]**.

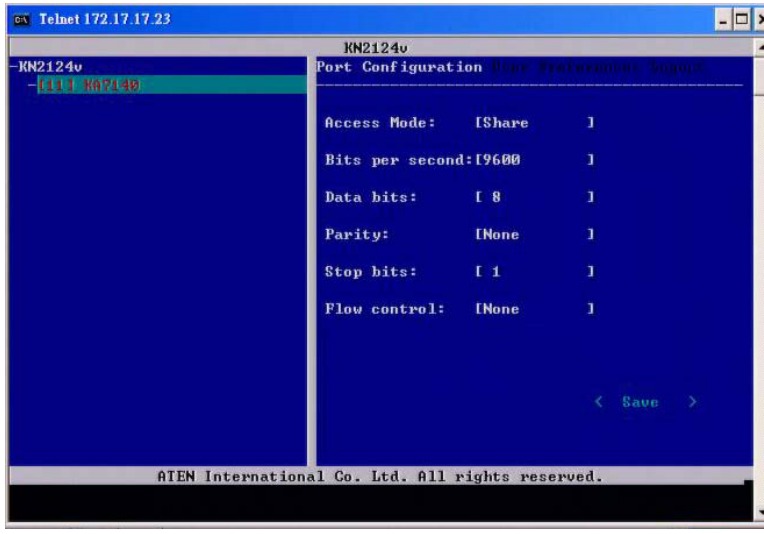
Switch Level Configuration

The right panel configuration settings that can be made when the KVM over IP switch is selected in the left panel are described in the table, below:

Setting	Description
Port Configuration	When Port Configuration is selected, press the Down Arrow key to highlight the current timeout figure. Key in a new timeout figure to overwrite the current one. **Note:** There is no way to erase the figure you key in. If you want to change it, use the Up Arrow key to leave the field, then, use Down Arrow to come back to it. After you come back, key in the new figure. When you have finished, use Down Arrow to highlight *Save*, then press **[Enter]**.
User Preferences	User Preferences lets you set a hotkey that brings you back to the access screen from the session you are working in. When User Preferences is selected, press the Down Arrow key to highlight the current hotkey letter. Key in the new letter to overwrite the current one. When you have finished, use Down Arrow to highlight *Save*, then press **[Enter]**.
Logout	When Logout is selected, press the Down Arrow key to highlight *Exit*, then press **[Enter]**.

Port Level Configuration

When a serial interface device is selected in the left panel, The screen looks similar to the one below:



The configuration settings that can be made when a serial interface device is selected are described in the table, below:

Setting	Description
Port Configuration	To configure the serial parameters: 1. Use the Up and Down Arrow keys to highlight the target item. 2. Press **[Enter]** to bring up the list of choices. 3. Use the Up and Down Arrow keys to highlight your choice, then press **[Enter]**. When you have finished, press the Down Arrow key to highlight *Save*, then press **[Enter]**.
User Preferences	User Preferences lets you set a hotkey that brings you back to the access screen from the session you are working in. When User Preferences is selected, press the Down Arrow key to highlight the current hotkey letter. Key in the new letter to overwrite the current one. When you have finished, use Down Arrow to highlight *Save*, then press **[Enter]**.
Logout	When Logout is selected, press the Down Arrow key to highlight *Exit*, then press **[Enter]**.

Additional Mouse Synchronization Procedures

If you use Manual Mouse Synchronization, you should perform the following operations on the servers that connect to the switch.

Note: 1. These procedures are to be performed on the servers attached to the switch's ports - not on the client computer you are using to access the KVM over IP switch.

2. In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the Windows operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

Windows:

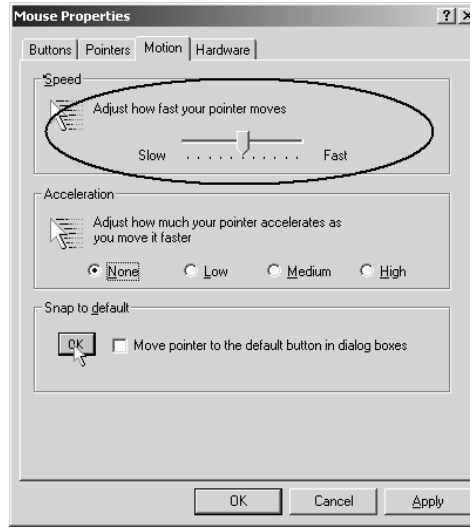
1. Windows 2000:

   a) Open the Mouse Properties dialog box (Control Panel → Mouse → Mouse Properties)

   b) Click the *Motion* tab

   c) Set the mouse speed to the middle position (6 units in from the left)

   d) Set the mouse acceleration to *None*



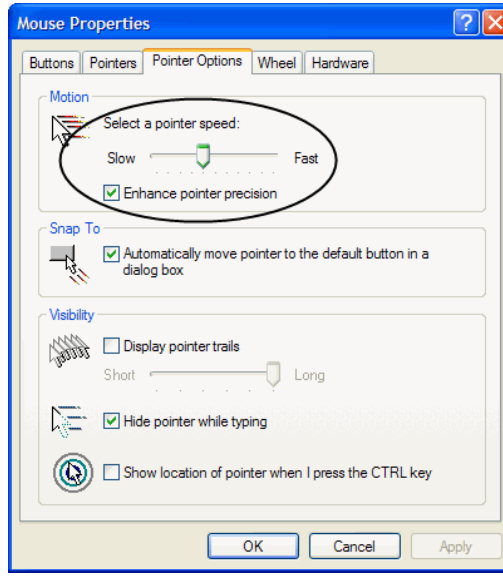
2. Windows XP / Windows Server 2003:

   a) Open the Mouse Properties dialog box (Control Panel → Mouse)

   b) Click the *Pointer Options* tab

   c) Set the mouse speed to the middle position (6 units in from the left)

   d) Disable *Enhance Pointer Precision*



3. Windows ME:

   Set the mouse speed to the middle position; disable mouse acceleration (click **Advanced** to get the dialog box for this).

4. Windows NT / Windows 98 / Windows 95:

   Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`
`or`
`xset m 1`

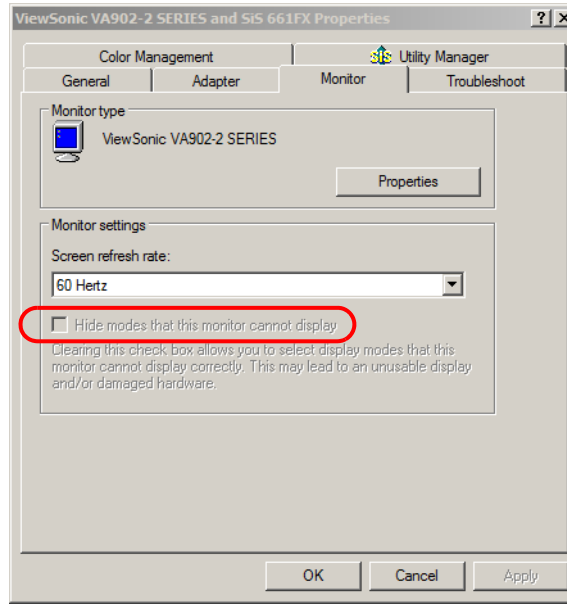
(If one doesn't help, try the other.)

Linux using the Redhat AS3.0 mouse mode: `xset m 1`

Additional Video Resolution Procedures

If you are running Windows, and wish to use new refresh rates, do the following:

1. Open Control Panel → Display → Settings → Advanced → Monitor.
2. In the dialog box that comes up, make sure that the *Hide modes that this monitor cannot display* checkbox is unchecked.



3. Click the arrow at the right of the *Screen refresh rate* listbox, and select the refresh rate you want from the list that appears.

Note: Make sure that your monitor supports the refresh rate you choose – if not, you may seriously damage your monitor.

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

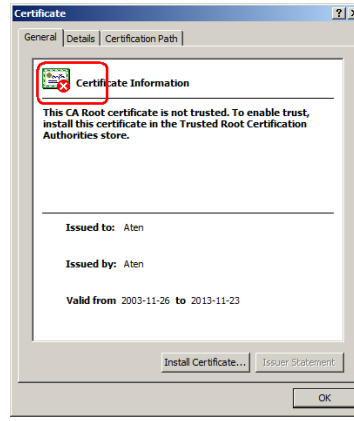
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

- If you are working on a client computer at another location, accept the certificate for just this session by clicking **Yes**.
- If you are working at your own client computer, install the certificate on your client computer (see below for details). After the certificate is installed, it will be recognized as trusted.

Installing the Certificate

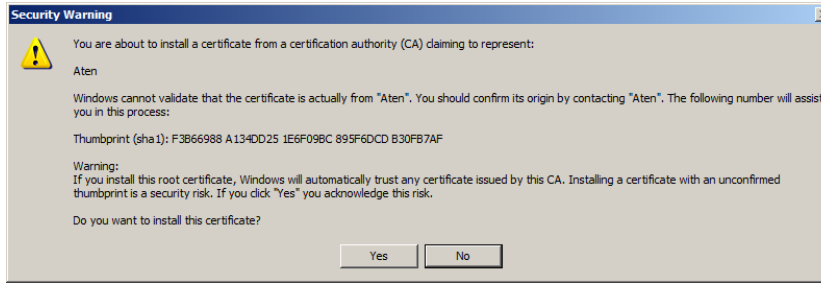
To install the certificate, do the following:

1. In the *Security Alert* dialog box, click **View Certificate.** The *Certificate Information* dialog box appears:



Note: There is a red and white **X** logo over the certificate to indicate that it is not trusted.

2. Click **Install Certificate**.
3. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.
4. When the Wizard presents a caution screen, click **Yes**.:


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
Aten
Windows cannot validate that the certificate is actually from "Aten". You should confirm its origin by contacting "Aten". The following number will assist you in this process:
Thumbprint (sha1): F3B66988 A134DD25 1E6F09BC 895F6DCD B30FB7AF
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

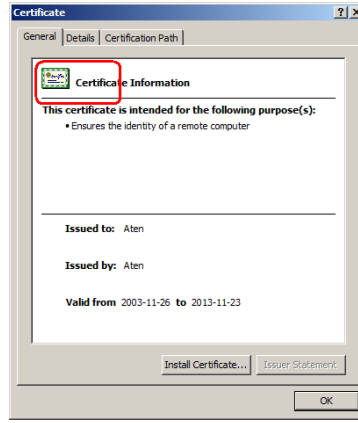
5. Click **Finish** to complete the installation; then click **OK** to close the dialog box.

Certificate Trusted

The certificate is now trusted:

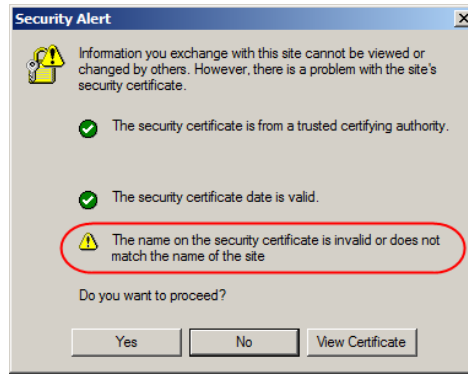
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

When you click *View Certificate*, you can see that the red and white **X** logo is no longer present – further indication that the certificate is trusted:



Mismatch Considerations

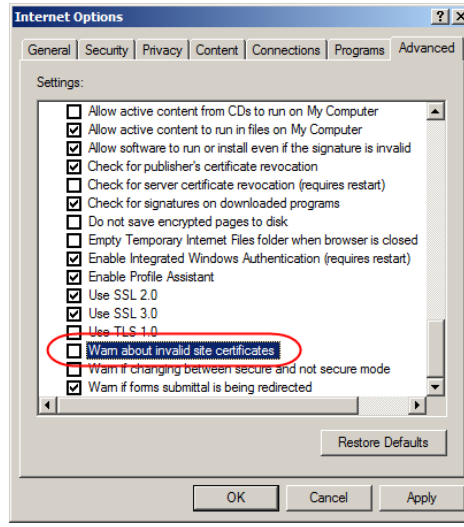
If the site name or IP address used for generating the certificate no longer matches the current address of the switch a mismatch warning occurs:


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

You can click **Yes** to go on, or you can disable mismatch checking.

To disable mismatch checking, do the following:

1. After the page you are logging in to comes up open the browser's Tools menu; Select *Internet Options* → *Advanced*.
2. Scroll to the bottom of the list and uncheck *Warn about trusted certificates*:


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings:
Allow active content from CDs to run on My Computer
Allow active content to run in files on My Computer
Allow software to run or install even if the signature is invalid
Check for publisher's certificate revocation
Check for server certificate revocation (requires restart)
Check for signatures on downloaded programs
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is closed
Enable Integrated Windows Authentication (requires restart)
Enable Profile Assistant
Use SSL 2.0
Use SSL 3.0
Use TLS 1.0
Warn about invalid site certificates
Warn if changing between secure and not secure mode
Warn if forms submittal is being redirected
Restore Defaults
OK
Cancel
Apply

3. Click **OK**. The next time you run the browser the change will be in effect.

Self-Signed Private Certificates

If you wish to create your own self-signed encryption key and certificate, a free utility – openssl.exe – is available for download over the web at **www.openssl.org**. To create your private key and certificate do the following:

1. Go to the directory where you downloaded and extracted *openssl.exe* to.
2. Run openssl.exe with the following parameters:

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf
```

Note: 1. The command should be entered all on one line (i.e., do not press [Enter] until all the parameters have been keyed in).

2. If there are spaces in the input, surround the entry in quotes (e.g., "ATEN International").

To avoid having to input information during key generation the following additional parameters can be used:

```
/C /ST /L /O /OU /CN /emailAddress.
```

Examples

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=yourcountry/ST=yourstateorprovince/L=yourlocationor
city/O=yourorganiztion/OU=yourorganizationalunit/
CN=yourcommonname/emailAddress=name@yourcompany.com
```

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=CA/ST=BC/L=Richmond/O="ATEN International"/OU=ATEN
/CN=ATEN/emailAddress=eservice@aten.com.tw
```

Importing the Files

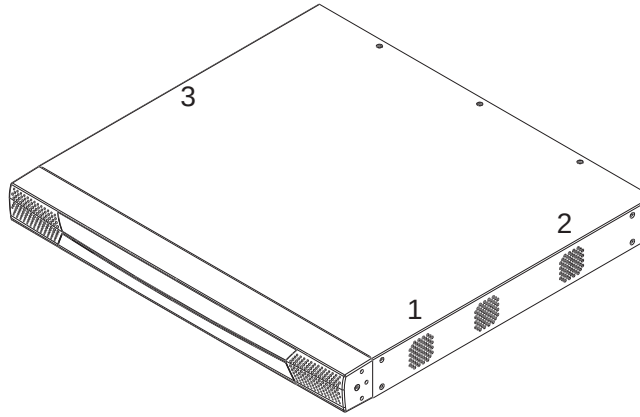
After the openssl.exe program completes, two files – CA.key (the private key) and CA.cer (the self-signed SSL certificate) – are created in the directory that you ran the program from. These are the files that you upload in the *Private Certificate* panel of the Security page (see *Security*, page 173, and *Private Certificate*, page 181).

Fan Location and Speed Information

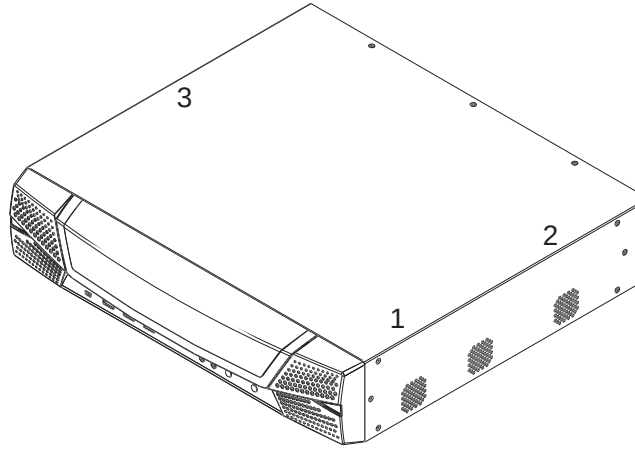
Fan Location

The KN8164V / KN8132V / KN4164V has 3 fans that feed real-time fan speed information to the WinClient / Java Client Device Management page.

KN8132V



KN8164V



The speed of each of the fans in the above image are shown on the *Device Information* web page. See page 153 for details.

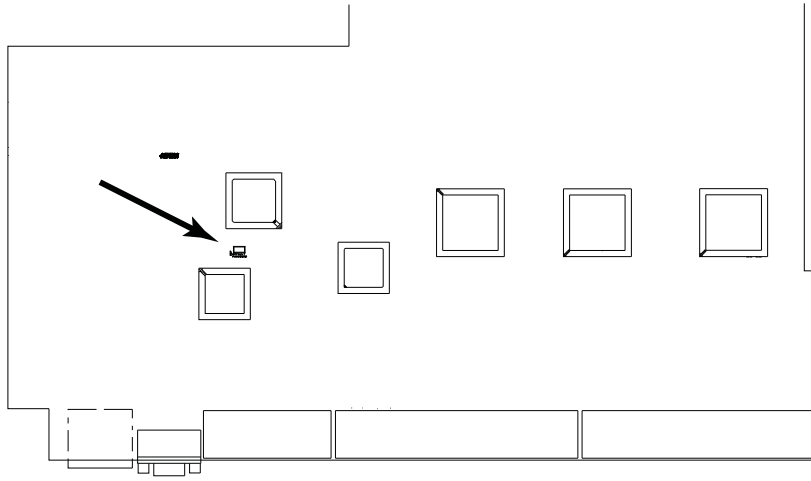
Clear Login Information

If you are unable to perform an Administrator login (because the Username and Password information has become corrupted or you have forgotten it, for example) you can clear the login information with the following procedure.

Note: Performing this procedure also returns all settings to their defaults.

To clear the login information (and return all settings to their defaults), do the following:

1. Power off the KVM over IP switch and remove its housing.
2. Use a jumper cap to short the mainboard jumper labeled **J25**.



3. Power on the switch.
4. When the Link and 10/100Mbps LEDs flash, power off the switch.
5. Remove the jumper cap from J25.
6. Close the housing and start the KVM over IP switch.

   After powering on the unit, you can use the default Super Administrator Username and Password (see *First Time Setup*, page 37), to log in.

Factory Default Settings

The default settings are as follows:

Setting	Default
Language	English
GUI Hotkey	[Scroll Lock] [Scroll Lock]
Port ID Display	Port Number + Name
Port ID Display Duration	3 Seconds
Scan Duration	5 Seconds
Screen Blanker	0 Minutes (disabled)
Beeper	On
Viewer	Auto Detect
Welcome Message	Hide
Accessible Ports	◆ Super Administrators – Full for all ports ◆ All other users – None for all ports.

Serial Adapter Pin Assignments

SA0142: RJ45-F to DB9-M (Black Connector) DTE to DCE

KVM over IP (RJ45)	Pins (8)		Modem/Device (DB9)
RTS	1	<——————>	7
DTR	2	<——————>	4
TXD	3	<——————>	3
CTS	4	<——————>	8
GND	5	<——————>	5
RXD	6	<——————>	2
DCD	7	<——————>	1
DSR	8	<——————>	6
			9 NC not used

Supported KVM Switches

The following is a list of fully supported KVM switches that can be used in a cascaded installation:

- KH88
- KH98
- KH1508
- KH1516
- KH1508A
- KH1516A
- CS9134
- CS9138

Note: 1. Some of the KVM over IP switch's features may not be supported, depending on the functionality of the cascaded KVM switch. (For example, some switches do not support virtual media.)

2. The installation cannot be cascaded beyond the second level.

Supported Power Over the Net™ Units

The following is a list of supported Power Over the Net™ units that can be connected to the KVM over IP switch:

- PN0108
- PN5212
- PN5320
- PN7212
- PN7320

Supported Power Distribution Units

The following is a list of fully supported PDU devices that can be connected to the KVM over IP switch:

- PE8r Series
- PE 9r Series

Virtual Media Support

WinClient ActiveX Viewer / WinClient AP

- IDE CDROM/DVD-ROM Drives – Read Only
- IDE Hard Drives – Read Only
- USB CDROM/DVD-ROM Drives – Read Only
- USB Hard Drives – Read/Write*
- USB Flash Drives – Read/Write*
- USB Floppy Drives – Read/Write
- Smart Card Readers – Read/Write (KA7166, KA7168, KA7169, KA7177 Adapter Cable only)

***** These drives can be mounted either as a Drive or as a Removable Disk (see *Virtual Media*, page 80). Removable disks allow the user to boot the remote server if the disk contains a bootable OS. In addition, if the disk contains more than one partition, the remote server can access all the partitions.

- ISO Files – Read Only
- Folders – Read/Write

Java Client Viewer / Java Client AP

- ISO Files – Read Only
- Folders – Read/Write

Limited Warranty

ALTUSEN warrants this product against defects in material or workmanship for a period of one (1) year from the date of purchase. If this product proves to be defective, contact ALTUSEN's support department for repair or replacement of your unit. ALTUSEN will not issue a refund. Return requests can not be processed without the original proof of purchase.

When returning the product, you must ship the product in its original packaging or packaging that gives an equal degree of protection. Include your proof of purchase in the packaging and the RMA number clearly marked on the outside of the package.

This warranty becomes invalid if the factory-supplied serial number has been removed or altered on the product.

This warranty does not cover cosmetic damage or damage due to acts of God, accident, misuse, abuse, negligence or modification of any part of the product. This warranty does not cover damage due to improper operation or maintenance, connection to improper equipment, or attempted repair by anyone other than ALTUSEN. This warranty does not cover products sold AS IS or WITH FAULTS.

IN NO EVENT SHALL ALTUSEN'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT. FURTHER, ALTUSEN SHALL NOT BE RESPONSIBLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. ALTUSEN SHALL NOT IN ANY WAY BE RESPONSIBLE FOR, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF PROFITS, DOWNTIME, GOODWILL, DAMAGE OR REPLACEMENT OF EQUIPMENT OR PROPERTY, AND ANY EXPENSES FROM RECOVERY, PROGRAMMING, AND REPRODUCTION OF ANY PROGRAM OR DATA.

ALTUSEN makes no warranty or representation, expressed, implied, or statutory with respect to its products, contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose.

ALTUSEN reserves the right to revise or update its product, software or documentation without obligation to notify any individual or entity of such revisions, or update.

For details about extended warranties, please contact one of our dedicated value added resellers.

Index

A

Access, 120
Access Ports, 158
Adapter cables
  firmware upgrade recovery, 202
Adapter connection diagram, 28, 29
Adapter ID Function, 34
Adding Users, 137
Additional Video Resolution Procedures, 267
ANMS, 162
AP GUI, 56
Array, 96
Associated Links, 129
Associating Ports
  blade servers, 110
associating ports, 110
Association
  Port/Outlet, 130
Authentication
  external, 162
Auto Scanning, 213
  Exiting, 214
  Invoking, 213
  Pausing, 214
  Scan Interval, 213
Auto scanning, 96

B

Backup, 203
Beeps, 154
Blade Association
  blade view, 111
  device view, 110
Blade Configuration, 110
Blade Configuration Page, 109
Blade Servers, 109, 188
Browser Login, 44

C

CC Management, 168
Certificate
  private, 181
  Signing Request, 182
Clear Login Information, 274
Components, 10
Configuration
  outlet, 131
Connecting
  Java Client AP, 51
  Windows Client AP, 47
Connection screen
  Java Client AP, 50
  Windows Client AP, 46
Connections
  KVM Devices/Ports, 101
Control Panel, 56
  Java Client AP, 92
  WinClient, 59
Create CSR, 182
Creating Groups, 142

D

Date/Time, 184
Deleting groups, 144
Deleting user accounts, 141
Device Assignment, 149
Device Management
  ANMS, 162
  Blade Servers, 188
  Date/Time, 184
  General, 154

KVM Devices, 153
Network, 157
OOBC, 170
Operating Mode, 155
PON Devices, 186
Security, 173
Device Monitor Page, 104
Device Permissions
assigning, 149, 152
Dial Back, 171
Dial Out, 171
DNS Server, 160, 161
DynaSync, 88

E

Event Panel, 228
Exit Macro, 127
External authentication, 162

F

Factory Default Settings, 275
Fan Location and Speed, 273
Fan Warning Message, 154
Favorites, 114
Features
V-Series exclusive, 6
Filter, 97, 192
Filtering
IP, 174
MAC, 174
Firmware
upgrading, 195
Firmware Upgrade
Main firmware, 196
Firmware upgrade recovery, 197

G

General page, 154
Groups
assigning users, 145, 147
creating, 142
Deleting, 144
Managing, 142
Modifying, 144
removing users, 146, 148
GUI
AP, 56

H

Hardware Setup, 15
History, 113
Hot Plugging, 32

I

Installation
Single Station, 25
Two Stage, 30
Introduction, 1
Invalid login, 43
IP
Address determination, 250
Filtering, 174
IP Installer, 158, 250
IPv4 Settings, 160
IPv6 Settings, 161

J

Java Client AP
Connecting, 51
Connection Screen, 50
Logging in, 49

K

KA7140 Pin Assignments, 261
KA7140 Setup and Operation, 259
Keyboard
On-Screen, 84

Keyboard Emulation
Mac, 255
Sun, 256
KVM configuration, 101

L

LDAP / LDAPS, 166
List Panel, 228
Local Console
GUI, 58
logging in, 43
Main Page, 58
Log, 191
filter, 192
Information page, 192
Notification Settings, 194
Log Server, 247
Configure, 223
Event Panel, 228
Events, 224
Installation, 221
List Panel, 228
Main Screen, 227
Menu Bar, 223
Options, 226
Starting Up, 222
Log server, 163, 221
Logging in
Browser, 44
Java Client AP, 49
Local console, 43
Windows Client AP, 45
Login
Invalid login, 43
Login Failures, 173
Login String, 177

M

MAC Filtering, 174
Mac Keyboard Emulation, 255
Macros
Search, 70
Main Firmware Upgrade, 196
Managing Groups, 142
Managing Users, 137
Message Board
Windows Client, 78
Mode, 180
Modem operation, 257
Modifying groups, 144
Modifying user accounts, 141
Module connection diagram, 28, 29
Mouse
DynaSync Mode, 88
Synchronization, 88
Mouse pointer type, 86
Mouse Problems, 241
Mouse synchronization
Windows, 265

N

Network page, 157
Network Time, 185
Network Transfer Rate, 161
NIC Settings, 159

O

Online
Registration, iv
On-Screen Keyboard, 84
OOBC, 170
Operating Mode, 155
Outlet Association, 130
Outlet Configuration, 131
Outlet Naming, 99
Outlet Schedule, 133
Outlet Settings, 108
Overview, 1

P

Panel array, 96
Panel Array Mode, 216, 247
Panel Array toolbar, 217
PON configuration, 104
PON Devices, 186
Port Access
  Access, 120
  blade servers, 109
  filter log, 192
  KVM devices, 93
  Sessions, 119
Port Access Page
  Recalling, 215
Port Association, 130
  synchronization, 134
Port Configuration, 126
Port Forwarding, 254
Port ID Numbering, 36
Port Naming, 99
Port Operation, 209
Port Properties
  Device Level, 126
  Port Level, 127
Port Selection, 36
  Sidebar, 95
Port Toolbar, 211
Ports
  connecting, 210
Power Management, 130
  Outlet configuration, 131
  Outlet schedule, 133
  synchronization, 134
Power Supply Detection, 154
Powering Off and Restarting, 35
PPP, 257
Private Certificate, 181
Private Certificates, 272

R

Rack Mounting
  Front, 17, 21
  Rear, 19, 23
RADIUS
  settings, 165
Redhat, 247
Redundant NIC, 159
refresh screen, 75
Requirements
  Operating Systems, 9
  OS Support, 9
Reset on exit, 206
Restore, 203
Restore Values, 206
RoHS, iii

S

Safety Instructions
  General, 229
  Rack Mounting, 231
Scan, 96
Schedule
  outlets, 133
screen, refresh, 75
Search
  Macros, 70
Security, 173
  Login string, 177
Self-signed certificates, 272
Serial Adapter pin assignments, 275
Serial Interface Configuration, 262
Sessions, 119
Sidebar
  ports/outlets, 95
Sidebar Utilities, 98
Single Station Installation, 25
SJ/T 11364-2006, iii

Skip Mode, 214
SSH, 158
Stacking, 16
Sun Keyboard Emulation, 256
Supported KVM Switches, 276
Synchronization, 134
  mouse, 88
System Requirements, 7
  KVM Adapter Cables, 8

T

Tab bar, 55
Technical Support, 236
Telephone support, iv
Time, 184
Toolbar
  Hotkey port switching, 213
  Icons, 212
  port switching, 211
Troubleshooting
  General Operation, 239
  Java Applet, 245
  Log Server, 247
  Mac Systems, 246
  Mouse problems, 241
  Panel Array Mode, 247
  Redhat, 247
  Sun Systems, 246
  Virtual Media, 243
  Web Browser, 243
  WinClient ActiveX Viewer, 244
  WinClient AP, 244
Trusted Certificates, 268
Two IP Addresses, 159
Two Stage Installation, 30

U

Unassociating Ports, 112
Upgrade firmware, 195
User Interface, 53
  Local Console, 58
  Tab bar, 55
  Web Browser Main Page, 53
User interface
  Page components, 54
User Management, 135
User Notice, v
Users
  Adding, 137
  assigning to groups, 145, 147
  Deleting, 141
  Managing, 137
  Modifying, 141
  removing from groups, 146, 148
Users and Groups, 145

V

Video Resolution
  additional procedures, 267
Video Settings, 73
Virtual Media
  icons, 80
  mounting, 80
  Troubleshooting, 243
  WinClient, 80
Virtual Media Support, 277

W

Warning beeps, 154
Web Browser Main Page, 53
Windows Client
  Auto Scanning, 213
  Message Board, 78
Windows Client AP
  Connecting, 47
  Connection Screen, 46
  File Menu, 48
  Logging in, 45